



# Atualize o seu sistema NetApp HCI versão 1,10 HCI

NetApp  
November 21, 2024

This PDF was generated from [https://docs.netapp.com/pt-br/hci/docs/concept\\_hci\\_upgrade\\_overview.html](https://docs.netapp.com/pt-br/hci/docs/concept_hci_upgrade_overview.html) on November 21, 2024. Always check docs.netapp.com for the latest.

# Índice

- Atualize o seu sistema NetApp HCI versão 1,10 ..... 1
  - Descrição geral da sequência de atualização ..... 1
  - Procedimentos de atualização do sistema ..... 2
- Atualize seus componentes vSphere para um sistema NetApp HCI com o plug-in Element para vCenter Server ..... 65

# Atualize o seu sistema NetApp HCI versão 1,10

## Descrição geral da sequência de atualização

Você pode manter seu sistema NetApp HCI atualizado após a implantação, atualizando sequencialmente todos os componentes de software NetApp HCI.

Esses componentes incluem serviços de gerenciamento, controle de nuvem híbrida NetApp, software Element, nó de gerenciamento, firmware de computação, drivers de computação e o plug-in Element para vCenter Server.



- A partir de novembro de 2023, você não pode iniciar uma atualização de componente usando o Controle de nuvem híbrida ou a API REST do NetApp porque os certificados de chave de assinatura (privados e públicos) expiraram em 5 de novembro de 2023. Você pode resolver esse problema seguindo a solução alternativa documentada no artigo da base de dados de Conhecimento ["As atualizações do SolidFire e HCI não podem ser iniciadas devido a um erro de carregamento do pacote de atualização"](#).
- A partir do Element 12,5, o NetApp HealthTools não é mais suportado para atualizações de software Element. Se você estiver executando o Element 11,0 ou 11,1, primeiro ["Atualize para o Element 12,3 usando HealthTools"](#) e depois atualize para o Element 12,5 ou posterior usando o Controle de nuvem híbrida da NetApp.

O [sequência de atualização do sistema](#) conteúdo descreve as tarefas necessárias para concluir uma atualização do sistema NetApp HCI. Idealmente, você executa esses procedimentos como parte da sequência de atualização maior e não isoladamente. Se for necessária uma atualização ou atualização baseada em componentes, consulte os pré-requisitos do procedimento para garantir que as complexidades adicionais sejam abordadas.

O [Sequência de atualização do vSphere](#) conteúdo do plug-in do Element para vCenter Server inclui etapas adicionais de pré e pós-atualização necessárias para reinstalar o plug-in do Element para o vCenter Server.

### O que você vai precisar

- Você está executando o nó de gerenciamento 11,3 ou posterior. As versões mais recentes do nó de gerenciamento têm uma arquitetura modular que fornece serviços individuais.



Para verificar a versão, faça login no nó de gerenciamento e veja o número da versão do elemento no banner de login. Se não tiver 11,3, ["Atualize seu nó de gerenciamento"](#) consulte

- Você atualizou seus serviços de gerenciamento para pelo menos a versão 2,1.326.

Os upgrades com o controle de nuvem híbrida da NetApp não estão disponíveis em versões anteriores do pacote de serviços.

- Você garantiu que a hora do sistema em todos os nós é sincronizada e que o NTP está configurado corretamente para o cluster de armazenamento e nós. Cada nó deve ser configurado com um servidor de nomes DNS na IU da Web por nó ([https://\[IP address\]:442](https://[IP address]:442)) sem falhas de cluster não resolvidas relacionadas ao desvio de tempo.
- Você agendou tempo suficiente para o ["Software Element"](#) e ["firmware de armazenamento"](#) upgrades. Quando você atualiza para o software Element 12,5 ou posterior, o tempo do processo de atualização varia dependendo da versão do software Element e das atualizações de firmware.

## sequência de atualização do sistema

Pode utilizar a seguinte sequência para atualizar o seu sistema NetApp HCI.

### Passos

1. ["Atualize os serviços de gerenciamento do Hybrid Cloud Control"](#).



Se você estiver atualizando os serviços de gerenciamento para a versão 2,16 ou posterior e estiver executando um nó de gerenciamento 11,3 a 11,8, precisará aumentar a RAM da VM do nó de gerenciamento antes de atualizar os serviços de gerenciamento.



Você deve atualizar para o pacote de serviços de gerenciamento mais recente antes de atualizar o software Element.

2. ["Execute verificações de integridade do storage Element antes de atualizar o storage"](#).

3. ["Atualize o software Element e o firmware de storage"](#).

4. ["\(Opcional\) Atualize apenas o firmware de armazenamento Element"](#).



Você pode executar esta tarefa quando uma nova atualização de firmware de armazenamento ficar disponível fora de uma versão principal.

5. ["\(Opcional\) Atualize seu nó de gerenciamento"](#).



A atualização do sistema operacional de nós de gerenciamento não é mais necessária para atualizar o software Element no cluster de storage. Se o nó de gerenciamento for a versão 11,3 ou posterior, você pode simplesmente atualizar os serviços de gerenciamento para a versão mais recente para executar atualizações de elementos usando o Controle de nuvem híbrida da NetApp. Siga o procedimento de atualização do nó de gerenciamento para o cenário se desejar atualizar o sistema operacional do nó de gerenciamento por outros motivos, como correção de segurança.

6. ["Atualize o plug-in Element para o vCenter Server"](#).

7. ["Execute verificações de integridade do nó de computação antes de atualizar o firmware da computação"](#).

8. ["Atualize seus drivers de nós de computação"](#).

9. ["Atualize o firmware do nó de computação usando o controle de nuvem híbrida da NetApp"](#) ou ["Automatize as atualizações de firmware de computação com o Ansible"](#).

### Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)
- ["Atualizar um sistema de storage all-flash NetApp SolidFire"](#)

## Procedimentos de atualização do sistema

## Atualizar serviços de gestão

Você pode atualizar seus serviços de gerenciamento para a versão mais recente do pacote depois de ter instalado o nó de gerenciamento 11,3 ou posterior.

A partir da versão do nó de gerenciamento do Element 11,3, o design do nó de gerenciamento foi alterado com base em uma nova arquitetura modular que fornece serviços individuais. Esses serviços modulares fornecem recursos de gerenciamento central e estendida para sistemas NetApp HCI. Os serviços de gerenciamento incluem serviços de telemetria, log e atualização do sistema, o serviço Qossoc para plug-in Element para vCenter Server, controle de nuvem híbrida NetApp e muito mais.

### Sobre esta tarefa

- Você deve atualizar para o pacote de serviços de gerenciamento mais recente antes de atualizar o software Element.



- Os serviços de gerenciamento 2.22.7 incluem o plug-in Element para vCenter Server 5,0 que contém o plug-in remoto. Se você usar o plug-in Element, você deve atualizar para os serviços de gerenciamento 2.22.7 ou posterior para cumprir com a diretiva VMware que remove o suporte para plug-ins locais. ["Saiba mais"](#).
- Para obter as notas de versão mais recentes dos serviços de gerenciamento que descrevem os principais serviços, novos recursos, correções de bugs e soluções alternativas para cada pacote de serviços, consulte ["notas de lançamento dos serviços de gerenciamento"](#)

### O que você vai precisar

A partir dos serviços de gerenciamento 2.20.69, você deve aceitar e salvar o Contrato de Licença de Usuário final (EULA) antes de usar a IU ou API do Controle de nuvem híbrida da NetApp para atualizar os serviços de gerenciamento:

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
3. Selecione **Upgrade** perto do canto superior direito da interface.
4. O EULA aparece. Role para baixo, selecione **Aceito para atualizações atuais e futuras** e selecione **Salvar**.

### Atualizar opções

Você pode atualizar os serviços de gerenciamento usando a IU do Controle de nuvem híbrida da NetApp ou a API REST do nó de gerenciamento:

- [Atualize os serviços de gerenciamento usando o Hybrid Cloud Control](#) (Método recomendado)
- [Atualize os serviços de gerenciamento usando a API do nó de gerenciamento](#)

### Atualize os serviços de gerenciamento usando o Hybrid Cloud Control

Você pode atualizar seus serviços de gerenciamento do NetApp usando o controle de nuvem híbrida da

NetApp.

Pacotes de serviços de gerenciamento fornecem funcionalidades aprimoradas e correções para sua instalação fora dos principais lançamentos.

### Antes de começar

- Você está executando o nó de gerenciamento 11,3 ou posterior.
- Se você estiver atualizando os serviços de gerenciamento para a versão 2,16 ou posterior e estiver executando um nó de gerenciamento 11,3 a 11,8, precisará aumentar a RAM da VM do nó de gerenciamento antes de atualizar os serviços de gerenciamento:
  - a. Desligue a VM do nó de gerenciamento.
  - b. Altere a RAM da VM do nó de gerenciamento de 12GB GB para 24GB GB de RAM.
  - c. Ligue a VM do nó de gerenciamento.
- A versão do cluster está executando o software NetApp Element 11,3 ou posterior.
- Você atualizou seus serviços de gerenciamento para pelo menos a versão 2,1.326. Os upgrades do controle de nuvem híbrida da NetApp não estão disponíveis em pacotes de serviços anteriores.



Para obter uma lista de serviços disponíveis para cada versão do pacote de serviços, consulte o ["Notas de versão dos Serviços de Gestão"](#).

### Passos

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
3. Selecione **Upgrade** perto do canto superior direito da interface.
4. Na página atualizações, selecione a guia **Serviços de gerenciamento**.
5. Siga as instruções na página para baixar e salvar um pacote de atualização de serviços de gerenciamento no computador.
6. Selecione Procurar para localizar o pacote que você salvou e carregá-lo.

Depois de carregar o pacote, a atualização é iniciada automaticamente.

Após o início da atualização, você pode ver o status da atualização nesta página. Durante a atualização, você pode perder a conexão com o Controle de nuvem híbrida da NetApp e ter que fazer login novamente para ver os resultados da atualização.

### Atualize os serviços de gerenciamento usando a API do nó de gerenciamento

Os usuários devem, idealmente, executar atualizações de serviços de gerenciamento a partir do Controle de nuvem híbrida da NetApp. No entanto, você pode fazer o upload, extrair e implantar manualmente uma atualização de pacote de serviços para os serviços de gerenciamento no nó de gerenciamento usando a API REST. Você pode executar cada comando a partir da IU da API REST para o nó de gerenciamento.

### Antes de começar

- Você implantou um nó de gerenciamento de software NetApp Element 11,3 ou posterior.
- Se você estiver atualizando os serviços de gerenciamento para a versão 2,16 ou posterior e estiver executando um nó de gerenciamento 11,3 a 11,8, precisará aumentar a RAM da VM do nó de gerenciamento antes de atualizar os serviços de gerenciamento:
  - a. Desligue a VM do nó de gerenciamento.
  - b. Altere a RAM da VM do nó de gerenciamento de 12GB GB para 24GB GB de RAM.
  - c. Ligue a VM do nó de gerenciamento.
- A versão do cluster está executando o software NetApp Element 11,3 ou posterior.
- Você atualizou seus serviços de gerenciamento para pelo menos a versão 2,1.326. Os upgrades do controle de nuvem híbrida da NetApp não estão disponíveis em pacotes de serviços anteriores.



Para obter uma lista de serviços disponíveis para cada versão do pacote de serviços, consulte o ["Notas de versão dos Serviços de Gestão"](#).

## Passos

1. Abra a IU da API REST no nó de gerenciamento:

`https://<ManagementNodeIP>/mnode`

2. Selecione **autorizar** e preencha o seguinte:
  - a. Introduza o nome de utilizador e a palavra-passe do cluster.
  - b. Introduza a ID do cliente como `mnode-client` se o valor ainda não estivesse preenchido.
  - c. Selecione **autorizar** para iniciar uma sessão.
  - d. Feche a janela.
3. Carregue e extraia o pacote de serviços no nó de gerenciamento usando este comando: `PUT /services/upload`
4. Implante os serviços de gerenciamento no nó de gerenciamento: `PUT /services/deploy`
5. Monitorize o estado da atualização: `GET /services/update/status`

Uma atualização bem-sucedida retorna um resultado semelhante ao seguinte exemplo:

```
{
  "current_version": "2.10.29",
  "details": "Updated to version 2.17.52",
  "status": "success"
}
```

## Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Execute verificações de integridade do storage Element antes de atualizar o storage

Você deve executar verificações de integridade antes de atualizar o storage Element para garantir que todos os nós de storage no cluster estejam prontos para a próxima atualização de storage Element.

### O que você vai precisar

- **Serviços de gerenciamento:** Você atualizou para o pacote de serviços de gerenciamento mais recente (2.10.27 ou posterior).



Você deve atualizar para o pacote de serviços de gerenciamento mais recente antes de atualizar o software Element.

- **Nó de gerenciamento:** Você está executando o nó de gerenciamento 11,3 ou posterior.
- **Software Element:** A versão do cluster está executando o software NetApp Element 11,3 ou posterior.
- **Contrato de Licença de Usuário final (EULA):** Começando com os serviços de gerenciamento 2.20.69, você deve aceitar e salvar o EULA antes de usar a IU ou API de Controle de nuvem híbrida da NetApp para executar verificações de integridade do armazenamento de elementos:
  - a. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

- b. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
- c. Selecione **Upgrade** perto do canto superior direito da interface.
- d. O EULA aparece. Role para baixo, selecione **Aceito para atualizações atuais e futuras** e selecione **Salvar**.

### Opções de verificação de integridade

Você pode executar verificações de integridade usando a IU do Controle de nuvem híbrida da NetApp ou a API de controle de nuvem híbrida da NetApp:

- [Use o controle de nuvem híbrida da NetApp para executar verificações de integridade do storage Element antes de atualizar o storage](#) (Método preferido)
- [Use a API para executar verificações de integridade do storage Element antes de atualizar o storage](#)

Você também pode saber mais sobre as verificações de integridade do storage executadas pelo serviço:

- [Verificações de integridade do armazenamento feitas pelo serviço](#)

### Use o controle de nuvem híbrida da NetApp para executar verificações de integridade do storage Element antes de atualizar o storage

Com o Controle de nuvem híbrida (HCC) da NetApp, você pode verificar se um cluster de storage está pronto para ser atualizado.

### Passos

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
3. Selecione **Upgrade** perto do canto superior direito da interface.
4. Na página **Upgrades**, selecione a guia **Storage**.
5. Selecione a verificação de integridade  do cluster que deseja verificar se há disponibilidade de atualização.
6. Na página **Verificação do estado do armazenamento**, selecione **Executar Verificação do estado**.
7. Se houver problemas, faça o seguinte:
  - a. Vá para o artigo específico da KB listado para cada problema ou execute o recurso especificado.
  - b. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.
  - c. Depois de resolver problemas de cluster, selecione **Re-Run Health Check**.

Depois que a verificação de integridade for concluída sem erros, o cluster de armazenamento estará pronto para ser atualizado. Consulte a atualização do nó de storage "[instruções](#)" para continuar.

### Use a API para executar verificações de integridade do storage Element antes de atualizar o storage

Você pode usar a API REST para verificar se um cluster de storage está pronto para ser atualizado. A verificação de integridade verifica se não há obstáculos na atualização, como nós pendentes, problemas de espaço em disco e falhas de cluster.

#### Passos

1. Localize a ID do cluster de armazenamento:
  - a. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/mnode
```

- b. Selecione **autorizar** e preencha o seguinte:
  - i. Introduza o nome de utilizador e a palavra-passe do cluster.
  - ii. Introduza a ID do cliente como `mnode-client` se o valor ainda não estivesse preenchido.
  - iii. Selecione **autorizar** para iniciar uma sessão.
  - iv. Feche a janela autorização.
- c. Na IU da API REST, `GET /assets` selecione .
- d. Selecione **Experimente**.
- e. Selecione **Executar**.
- f. A partir da resposta, copie o "id" da "storage" seção do cluster que você pretende verificar a disponibilidade da atualização.



Não use o "parent" valor nesta seção porque esta é a ID do nó de gerenciamento, não a ID do cluster de armazenamento.

```
"config": {},
"credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",
"host_name": "SF_DEMO",
"\"id\": \"12cc3a45-e6e7-8d91-a2bb-0bdb3456b789\",
"ip": "10.123.12.12",
"parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",
"sshcredentialid": null,
"ssl_certificate": null
```

2. Execute verificações de integridade no cluster de armazenamento:

a. Abra a IU da API REST de storage no nó de gerenciamento:

```
https://<ManagementNodeIP>/storage/1/
```

b. Selecione **autorizar** e preencha o seguinte:

- i. Introduza o nome de utilizador e a palavra-passe do cluster.
- ii. Introduza a ID do cliente como `mnode-client` se o valor ainda não estivesse preenchido.
- iii. Selecione **autorizar** para iniciar uma sessão.
- iv. Feche a janela autorização.

c. Selecione **POST /Health-checks**.

d. Selecione **Experimente**.

e. No campo Parameter (parâmetro), introduza a ID do cluster de armazenamento obtida no passo 1.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

f. Selecione **execute** para executar uma verificação de integridade no cluster de armazenamento especificado.

A resposta deve indicar o estado `initializing`:

```

{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}

```

- a. Copie `healthCheckID` o que faz parte da resposta.
3. Verificar os resultados das verificações de saúde:
    - a. Selecione **GET /health-checks/(healthCheckId)**.
    - b. Selecione **Experimente**.
    - c. Introduza a ID da verificação de integridade no campo parâmetro.
    - d. Selecione **Executar**.
    - e. Role até a parte inferior do corpo de resposta.

Se todas as verificações de integridade forem bem-sucedidas, o retorno será semelhante ao seguinte exemplo:

```

"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"

```

4. Se o `message` retorno indicar que houve problemas em relação à integridade do cluster, faça o seguinte:
  - a. Selecione **GET /health-checks/(healthCheckId/log)**
  - b. Selecione **Experimente**.
  - c. Introduza a ID da verificação de integridade no campo parâmetro.
  - d. Selecione **Executar**.
  - e. Revise quaisquer erros específicos e obtenha os links de artigos da KB associados.
  - f. Vá para o artigo específico da KB listado para cada problema ou execute o recurso especificado.
  - g. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.

h. Depois de resolver problemas de cluster, execute **GET /Health-checks//log** novamente.

### Verificações de integridade do armazenamento feitas pelo serviço

As verificações de integridade do armazenamento fazem as seguintes verificações por cluster.

Nome de verificação	Nó/cluster	Descrição
check_async_results	Cluster	Verifica se o número de resultados assíncronos no banco de dados está abaixo de um número de limite.
check_cluster_faults	Cluster	Verifica se não há falhas de cluster de bloqueio de atualização (conforme definido na fonte do elemento).
check_upload_speed	Nó	Mede a velocidade de upload entre o nó de armazenamento e o nó de gerenciamento.
connection_speed_check	Nó	Verifica se os nós têm conectividade com o nó de gerenciamento que serve pacotes de atualização e estima a velocidade da conexão.
check_cores	Nó	Verifica o despejo de falhas do kernel e arquivos de núcleo no nó. A verificação falha para qualquer falha em um período de tempo recente (limite de 7 dias).
check_root_disk_space	Nó	Verifica se o sistema de arquivos raiz tem espaço livre suficiente para executar uma atualização.
check_var_log_disk_space	Nó	Verifica se <code>/var/log</code> o espaço livre atende a algum limite de porcentagem livre. Se não o fizer, a verificação irá rodar e purgar os registros mais antigos, de forma a ficar abaixo do limite. A verificação falha se não for bem sucedida em criar espaço livre suficiente.
check_pending_nodes	Cluster	Verifica se não há nós pendentes no cluster.

### Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Atualize o software Element

Para atualizar o software NetApp Element, você pode usar a IU ou a API REST do NetApp Hybrid Cloud Control. Certas operações são suprimidas durante uma atualização do software Element, como adicionar e remover nós, adicionar e remover unidades, e comandos associados a iniciadores, grupos de acesso de volume e redes virtuais, entre outros.



A partir do Element 12,5, o NetApp HealthTools não é mais suportado para atualizações de software Element. Se você estiver executando o Element 11,0 ou 11,1, primeiro ["Atualize para o Element 12,3 usando HealthTools"](#) e depois atualize para o Element 12,5 ou posterior usando o Controle de nuvem híbrida da NetApp.

### O que você vai precisar

- **Admin Privileges:** Você tem permissões de administrador de cluster de armazenamento para executar a atualização.
- **Caminho de atualização válido:** Você verificou as informações do caminho de atualização para a versão do Element para a qual está atualizando e verificou que o caminho de atualização é válido. Consulte ["NetApp KB: Matriz de atualização para clusters de armazenamento que executam o software NetApp Element"](#)
- **Sincronização da hora do sistema:** Você garantiu que a sincronização da hora do sistema em todos os nós e que o NTP está configurado corretamente para o cluster de armazenamento e nós. Cada nó deve ser configurado com um servidor de nomes DNS na IU da Web por nó (`https://[IP address]:442`) sem falhas de cluster não resolvidas relacionadas ao desvio de tempo.
- **Portas do sistema:** Se você estiver usando o Controle de nuvem híbrida da NetApp para atualizações, você garantiu que as portas necessárias estejam abertas. Consulte ["Portas de rede"](#) para obter mais informações.
- **Nó de gerenciamento:** Para a API e a IU do NetApp Hybrid Cloud Control, o nó de gerenciamento em seu ambiente está executando a versão 11,3.
- **Serviços de gerenciamento:** Você atualizou seu pacote de serviços de gerenciamento para a versão mais recente.



Você deve atualizar para o pacote de serviços de gerenciamento mais recente antes de atualizar o software Element para a versão 12,5 ou posterior. Se você estiver atualizando o software Element para a versão 12,5 ou posterior, precisará dos serviços de gerenciamento 2.21.61 ou posterior para continuar.

- **Integridade do cluster:** Você verificou que o cluster está pronto para ser atualizado. ["Execute verificações de integridade do storage Element antes de atualizar o storage"](#) Consulte .
- \* Controlador de gerenciamento de placa base (BMC) atualizado para H610S nós\*: Você atualizou a versão do BMC para seus H610S nós. Consulte ["notas de versão e instruções de atualização"](#).
- **Tempo de processo de atualização:** Você agendou tempo suficiente para realizar a atualização. Quando você atualiza para o software Element 12,5 ou posterior, o tempo do processo de atualização varia dependendo da versão atual do software Element e das atualizações de firmware.

Nó de storage	Versão atual do software Element	O tempo aproximado de instalação de software e firmware por nó 1	O tempo aproximado de sincronização de dados por nó 2	Tempo total aproximado de atualização por nó
Todos os nós da série H SolidFire e NetApp com firmware atualizado	12.x	15 minutos	10 a 15 minutos	20 a 30 minutos
H610S e H410S	12.x e 11,8	60 minutos	30 a 60 minutos	90 a 120 minutos
H610S	11,7 e anteriores	90 minutos	40 a 70 minutos	De 130 a 160 minutos, você também precisa "execute um desligamento completo do nó e desconexão de energia" para cada nó H610S.

1 para obter uma matriz completa de firmware e firmware de driver para o seu hardware, "[Versões de firmware e driver ESXi compatíveis para versões de NetApp HCI e firmware para nós de storage NetApp HCI](#)" consulte .

2 se você combinar um cluster com uma carga de IOPS de gravação pesada com um tempo de atualização de firmware mais longo, o tempo de sincronização de dados aumentará.

- **Contrato de Licença de Usuário final (EULA):** Começando com os serviços de gerenciamento 2.20.69, você deve aceitar e salvar o EULA antes de usar a interface de usuário ou API do NetApp Hybrid Cloud Control para atualizar o software Element:

a. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

- b. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
- c. Selecione **Upgrade** perto do canto superior direito da interface.
- d. O EULA aparece. Role para baixo, selecione **Aceito para atualizações atuais e futuras** e selecione **Salvar**.

### Opções de atualização

Escolha uma das seguintes opções de atualização do software Element:

- [Use a IU do Controle de nuvem híbrida da NetApp para atualizar o storage Element](#)
- [Use a API de controle de nuvem híbrida da NetApp para atualizar o storage Element](#)



Se você estiver atualizando um nó da série H610S para o elemento 12,5 ou posterior e o nó estiver executando uma versão do software Element anterior a 11,8, será necessário executar as etapas de atualização adicionais "[Artigo da KB](#)" para cada nó de storage. Se você estiver executando o Element 11,8 ou posterior, as etapas adicionais de atualização não serão necessárias.

## Use a IU do Controle de nuvem híbrida da NetApp para atualizar o storage Element

Usando a IU do Controle de nuvem híbrida da NetApp, você pode atualizar um cluster de storage.



Para possíveis problemas durante a atualização dos clusters de storage usando o Controle de nuvem híbrida da NetApp e suas soluções alternativas, consulte este "[Artigo da KB](#)".

### Passos

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
3. Selecione **Upgrade** perto do canto superior direito da interface.
4. Na página **Upgrades**, selecione **Storage**.

A guia **Storage** lista os clusters de armazenamento que fazem parte da sua instalação. Se um cluster estiver inacessível pelo Controle de nuvem híbrida da NetApp, ele não será exibido na página **Upgrades**.

5. Escolha entre as opções a seguir e execute o conjunto de etapas aplicáveis ao cluster:

Opção	Passos
<p>Todos os clusters executando o elemento 11,8 e posterior</p>	<p>a. Selecione <b>Procurar</b> para carregar o pacote de atualização que transferiu.</p> <p>b. Aguarde até que o upload seja concluído. Uma barra de progresso mostra o status do upload.</p> <div data-bbox="922 373 976 432" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 352 1455 453" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>O upload do arquivo será perdido se você navegar para longe da janela do navegador.</p> </div> <p>É apresentada uma mensagem no ecrã depois de o ficheiro ser carregado e validado com êxito. A validação pode demorar vários minutos. Se você navegar para longe da janela do navegador nesta fase, o upload do arquivo será preservado.</p> <p>c. Selecione <b>Begin Upgrade</b>.</p> <div data-bbox="922 940 976 999" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 814 1455 1117" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>O <b>Status do Upgrade</b> muda durante a atualização para refletir o status do processo. Ele também muda em resposta às ações que você toma, como pausar a atualização, ou se a atualização retornar um erro. <a href="#">Alterações de status da atualização</a> Consulte .</p> </div> <div data-bbox="922 1339 976 1398" style="display: inline-block; vertical-align: middle; margin-top: 20px;">  </div> <div data-bbox="1036 1171 1455 1545" style="display: inline-block; vertical-align: middle; margin-left: 10px; margin-top: 20px;"> <p>Enquanto a atualização estiver em andamento, você pode sair da página e voltar a ela mais tarde para continuar monitorando o progresso. A página não atualiza dinamicamente o status e a versão atual se a linha do cluster for recolhida. A linha do cluster deve ser expandida para atualizar a tabela ou você pode atualizar a página.</p> </div> <p>Pode transferir registos após a conclusão da atualização.</p>

Opção	Passos
Você está atualizando um cluster H610S executando a versão do Element anterior a 11,8.	<p>a. Selecione a seta suspensa ao lado do cluster que você está atualizando e selecione a partir das versões de atualização disponíveis.</p> <p>b. Selecione <b>Begin Upgrade</b>. Após a conclusão da atualização, a IU solicitará que você execute etapas adicionais de atualização.</p> <p>c. Conclua as etapas adicionais necessárias no "Artigo da KB" e confirme na IU que você as concluiu.</p> <p>Pode transferir registros após a conclusão da atualização. Para obter informações sobre as várias alterações de status de atualização, <a href="#">Alterações de status da atualização</a> consulte .</p>

### Alterações de status da atualização

Aqui estão os diferentes estados que a coluna **Status da atualização** na IU mostra antes, durante e após o processo de atualização:

Estado de atualização	Descrição
Atualizado	O cluster foi atualizado para a versão mais recente do Element disponível.
Versões disponíveis	Versões mais recentes do Element e/ou firmware de storage estão disponíveis para atualização.
Em curso	A atualização está em andamento. Uma barra de progresso mostra o status da atualização. As mensagens na tela também mostram falhas no nível do nó e exibem a ID do nó de cada nó no cluster à medida que a atualização progride. Você pode monitorar o status de cada nó usando a IU do Element ou o plug-in do NetApp Element para a IU do vCenter Server.
Atualizar Pausando	Você pode optar por pausar a atualização. Dependendo do estado do processo de atualização, a operação de pausa pode ser bem-sucedida ou falhar. Você verá um prompt da interface do usuário solicitando que você confirme a operação de pausa. Para garantir que o cluster esteja em um local seguro antes de pausar uma atualização, pode levar até duas horas para que a operação de atualização seja completamente pausada. Para retomar a atualização, selecione <b>Resume</b> .
Em pausa	Fez uma pausa na atualização. Selecione <b>Resume</b> para retomar o processo.

Estado de atualização	Descrição
Erro	Ocorreu um erro durante a atualização. Você pode baixar o log de erros e enviá-lo para o suporte da NetApp. Depois de resolver o erro, você pode retornar à página e selecionar <b>Resume</b> . Quando você retoma a atualização, a barra de progresso recua por alguns minutos enquanto o sistema executa a verificação de integridade e verifica o estado atual da atualização.
Completo com acompanhamento	Somente para nós H610S atualizando a partir da versão do Element anterior à 11,8. Após a conclusão da fase 1 do processo de atualização, este estado solicita que você execute etapas adicionais de atualização (consulte a " <a href="#">Artigo da KB</a> "). Depois de concluir estes passos adicionais e confirmar que o concluiu, o estado muda para <b>até à data</b> .

## Use a API de controle de nuvem híbrida da NetApp para atualizar o storage Element

Você pode usar APIs para atualizar nós de storage em um cluster para a versão mais recente do software Element. Você pode usar uma ferramenta de automação de sua escolha para executar as APIs. O fluxo de trabalho da API documentado aqui usa a IU da API REST disponível no nó de gerenciamento como exemplo.

### Passos

1. Faça download do pacote de atualização de storage para um dispositivo que esteja acessível ao nó de gerenciamento; vá para o software NetApp HCI "[página de transferências](#)" e baixe a imagem mais recente do nó de storage.
2. Faça o upload do pacote de atualização de armazenamento para o nó de gerenciamento:
  - a. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
    - i. Introduza o nome de utilizador e a palavra-passe do cluster.
    - ii. Introduza a ID do cliente como `mnode-client`.
    - iii. Selecione **autorizar** para iniciar uma sessão.
    - iv. Feche a janela autorização.
  - c. Na IU da API REST, selecione **POST /packages**.
  - d. Selecione **Experimente**.
  - e. Selecione **Procurar** e selecione o pacote de atualização.
  - f. Selecione **execute** para iniciar o upload.
  - g. Na resposta, copie e salve o ID do ("id" pacote ) para uso em uma etapa posterior.
3. Verifique o status do upload.
    - a. Na IU da API REST, selecione **GET /packages/ id/status**.
    - b. Selecione **Experimente**.

- c. Insira o ID do pacote que você copiou na etapa anterior em **id**.
- d. Selecione **execute** para iniciar a solicitação de status.

A resposta indica `state` como `SUCCESS` quando concluída.

4. Localize a ID do cluster de armazenamento:

- a. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selecione **autorizar** e preencha o seguinte:

- i. Introduza o nome de utilizador e a palavra-passe do cluster.
- ii. Introduza a ID do cliente como `mnode-client`.
- iii. Selecione **autorizar** para iniciar uma sessão.
- iv. Feche a janela autorização.

- c. Na IU da API REST, selecione **GET /installations**.

- d. Selecione **Experimente**.

- e. Selecione **Executar**.

- f. Na resposta, copie o ID do ativo de instalação ("`id`").

- g. Na IU da API REST, selecione **\*GET /installations/**

- h. Selecione **Experimente**.

- i. Cole o ID do ativo de instalação no campo **id**.

- j. Selecione **Executar**.

- k. A partir da resposta, copie e salve o ID do cluster de armazenamento ("`id`") do cluster que pretende atualizar para uso em uma etapa posterior.

5. Execute a atualização de armazenamento:

- a. Abra a IU da API REST de storage no nó de gerenciamento:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Selecione **autorizar** e preencha o seguinte:

- i. Introduza o nome de utilizador e a palavra-passe do cluster.
- ii. Introduza a ID do cliente como `mnode-client`.
- iii. Selecione **autorizar** para iniciar uma sessão.
- iv. Feche a janela autorização.

- c. Selecione **POST /Upgrades**.

- d. Selecione **Experimente**.

- e. Introduza a ID do pacote de atualização no campo **Parameter** (parâmetro).

f. Introduza a ID do cluster de armazenamento no campo Parameter (parâmetro).

A carga útil deve ser semelhante ao seguinte exemplo:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. Selecione **execute** para iniciar a atualização.

A resposta deve indicar o estado como `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1",
    "log": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1/log"
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {

```

```
    "checkID": 0,  
    "name": "string",  
    "displayName": "string",  
    "passed": true,  
    "kb": "string",  
    "description": "string",  
    "remedy": "string",  
    "severity": "string",  
    "data": {},  
    "nodeID": 0  
  }  
]  
,  
"taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",  
"dateCompleted": "2020-04-21T22:10:57.057Z",  
"dateCreated": "2020-04-21T22:10:57.057Z"  
}
```

- a. Copie o ID de atualização ("upgradeId") que faz parte da resposta.
6. Verifique o progresso e os resultados da atualização:
- a. Selecione \*GET /Upgrades/
  - b. Selecione **Experimente**.
  - c. Insira o ID de atualização da etapa anterior em **upgradeId**.
  - d. Selecione **Executar**.
  - e. Siga um destes procedimentos se houver problemas ou requisitos especiais durante a atualização:

Opção	Passos
<p>Você precisa corrigir problemas de integridade do cluster devido a <code>failedHealthChecks</code> mensagem no corpo de resposta.</p>	<ol style="list-style-type: none"> <li>i. Vá para o artigo específico da KB listado para cada problema ou execute o recurso especificado.</li> <li>ii. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.</li> <li>iii. Depois de resolver problemas de cluster, reautentique se necessário e selecione <code>*put /Upgrades/</code></li> <li>iv. Selecione <b>Experimente</b>.</li> <li>v. Insira o ID de atualização da etapa anterior em <code>upgradedId</code>.</li> <li>vi. Introduza <code>"action": "resume"</code> o corpo do pedido. <div data-bbox="915 716 1487 896" style="border: 1px solid #ccc; border-radius: 5px; padding: 10px; margin: 10px 0;"> <pre>{   "action": "resume" }</pre> </div> </li> <li>vii. Selecione <b>Executar</b>.</li> </ol>
<p>Você precisa pausar a atualização porque a janela de manutenção está fechando ou por outro motivo.</p>	<ol style="list-style-type: none"> <li>i. Reautentique se necessário e selecione <code>*put /Upgrades/</code></li> <li>ii. Selecione <b>Experimente</b>.</li> <li>iii. Insira o ID de atualização da etapa anterior em <code>upgradedId</code>.</li> <li>iv. Introduza <code>"action": "pause"</code> o corpo do pedido. <div data-bbox="915 1333 1487 1514" style="border: 1px solid #ccc; border-radius: 5px; padding: 10px; margin: 10px 0;"> <pre>{   "action": "pause" }</pre> </div> </li> <li>v. Selecione <b>Executar</b>.</li> </ol>

Opção	Passos
<p>Se você estiver atualizando um cluster H610S executando uma versão do Element anterior a 11,8, verá o estado <code>finishedNeedsAck</code> no corpo da resposta. Você deve executar etapas de atualização adicionais para cada nó de storage do H610S.</p>	<ol style="list-style-type: none"> <li>i. Conclua as etapas adicionais de atualização "<a href="#">Artigo da KB</a>" para cada nó.</li> <li>ii. Reautentique se necessário e selecione <code>*put /Upgrades/</code></li> <li>iii. Selecione <b>Experimente</b>.</li> <li>iv. Insira o ID de atualização da etapa anterior em <b>upgradeld</b>.</li> <li>v. Introduza <code>"action": "acknowledge"</code> o corpo do pedido. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>{   "action": "acknowledge" }</pre> </div> </li> <li>vi. Selecione <b>Executar</b>.</li> </ol>

- f. Execute a API **GET /Upgrades/"upgradeld"** várias vezes, conforme necessário, até que o processo esteja concluído.

Durante a atualização, o `status` indica `running` se não foram encontrados erros. À medida que cada nó é atualizado, o `step` valor muda para `NodeFinished`.

A atualização foi concluída com êxito quando o `percent` valor é 100 e o `state` indica `finished`.

### O que acontece se uma atualização falhar usando o controle de nuvem híbrida da NetApp

Se uma unidade ou nó falhar durante uma atualização, a IU do Element mostrará falhas de cluster. O processo de atualização não avança para o nó seguinte e aguarda a resolução das falhas do cluster. A barra de progresso na IU mostra que a atualização está aguardando a resolução das falhas do cluster. Nesta fase, selecionar **Pausa** na IU não funcionará, porque a atualização aguarda que o cluster esteja saudável. Você precisará ativar o suporte da NetApp para ajudar na investigação de falha.

O controle de nuvem híbrida da NetApp tem um período de espera pré-definido de três horas, durante o qual um dos seguintes cenários pode acontecer:

- As falhas do cluster são resolvidas dentro da janela de três horas e a atualização é retomada. Você não precisa tomar nenhuma ação nesse cenário.
- O problema persiste após três horas e o status da atualização mostra **erro** com um banner vermelho. Você pode retomar a atualização selecionando **Resume** após o problema ser resolvido.
- O suporte da NetApp determinou que a atualização precisa ser temporariamente cancelada para tomar medidas corretivas antes da janela de três horas. O suporte usará a API para cancelar a atualização.



Abortar a atualização do cluster enquanto um nó está sendo atualizado pode resultar na remoção desgraciosa das unidades do nó. Se as unidades forem removidas sem graça, adicionar as unidades de volta durante uma atualização exigirá intervenção manual pelo suporte da NetApp. O nó pode estar demorando mais para fazer atualizações de firmware ou atividades de sincronização pós-atualização. Se o progresso da atualização parecer interrompido, entre em Contato com o suporte da NetApp para obter assistência.

## Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Atualize o firmware de armazenamento

A partir do Element 12,0 e dos serviços de gerenciamento versão 2,14, é possível fazer atualizações somente de firmware nos nós de storage usando a IU e a API REST do NetApp Hybrid Cloud Control. Esse procedimento não atualiza o software Element e permite que você atualize o firmware de storage fora de uma versão do elemento principal.

### O que você vai precisar

- **Admin Privileges:** Você tem permissões de administrador de cluster de armazenamento para executar a atualização.
- **Sincronização da hora do sistema:** Você garantiu que a sincronização da hora do sistema em todos os nós e que o NTP está configurado corretamente para o cluster de armazenamento e nós. Cada nó deve ser configurado com um servidor de nomes DNS na IU da Web por nó ([https://\[IP address\]:442](https://[IP address]:442)) sem falhas de cluster não resolvidas relacionadas ao desvio de tempo.
- **Portas do sistema:** Se você estiver usando o Controle de nuvem híbrida da NetApp para atualizações, você garantiu que as portas necessárias estejam abertas. Consulte ["Portas de rede"](#) para obter mais informações.
- **Nó de gerenciamento:** Para a API e a IU do NetApp Hybrid Cloud Control, o nó de gerenciamento em seu ambiente está executando a versão 11,3.
- **Serviços de gerenciamento:** Você atualizou seu pacote de serviços de gerenciamento para a versão mais recente.



Para H610S nós de storage que executam o software Element versão 12,0, você deve aplicar o D-patch SUST-909 antes de atualizar para o pacote de firmware de storage 2,27. Entre em Contato com o suporte da NetApp para obter o D-patch antes de atualizar. ["Notas de lançamento do pacote de firmware de armazenamento 2,27"](#) Consulte .



É necessário atualizar para o pacote de serviços de gerenciamento mais recente antes de atualizar o firmware nos nós de storage. Se você estiver atualizando o software Element para a versão 12,2 ou posterior, precisará dos serviços de gerenciamento 2.14.60 ou posterior para continuar.



Para atualizar o firmware do iDRAC/BIOS, entre em Contato com o suporte da NetApp. Para obter informações adicionais, consulte este ["Artigo da KB"](#).

- **Cluster Health:** Você executou verificações de integridade. "[Execute verificações de integridade do storage Element antes de atualizar o storage](#)"Consulte .
- \* Controlador de gerenciamento de placa base (BMC) atualizado para H610S nós\*: Você atualizou a versão do BMC para seus H610S nós. "[notas de versão e instruções de atualização](#)"Consulte .



Para obter uma matriz completa de firmware e firmware de driver para seu hardware, "[Versões de firmware compatíveis para nós de storage do NetApp HCI](#)" consulte .

- **Tempo de processo de atualização:** Você agendou tempo suficiente para realizar a atualização. Quando você atualiza para o software Element 12,5 ou posterior, o tempo do processo de atualização varia dependendo da versão atual do software Element e das atualizações de firmware.

Nó de storage	Versão atual do software Element	O tempo aproximado de instalação de software e firmware por nó 1	O tempo aproximado de sincronização de dados por nó 2	Tempo total aproximado de atualização por nó
Todos os nós da série H SolidFire e NetApp com firmware atualizado	12.x	15 minutos	10 a 15 minutos	20 a 30 minutos
H610S e H410S	12.x e 11,8	60 minutos	30 a 60 minutos	90 a 120 minutos
H610S	11,7 e anteriores	90 minutos	40 a 70 minutos	De 130 a 160 minutos, você também precisa " <a href="#">execute um desligamento completo do nó e desconexão de energia</a> " para cada nó H610S.

1 para obter uma matriz completa de firmware e firmware de driver para o seu hardware, "[Versões de firmware e driver ESXi compatíveis para versões de NetApp HCI e firmware para nós de storage NetApp HCI](#)"consulte .

2 se você combinar um cluster com uma carga de IOPS de gravação pesada com um tempo de atualização de firmware mais longo, o tempo de sincronização de dados aumentará.

- **Contrato de Licença de Usuário final (EULA):** Começando com os serviços de gerenciamento 2.20.69, você deve aceitar e salvar o EULA antes de usar a interface ou API do Controle de nuvem híbrida da NetApp para atualizar o firmware de armazenamento:

- Abra o endereço IP do nó de gerenciamento em um navegador da Web:

`https://<ManagementNodeIP>`

- Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.

- c. Selecione **Upgrade** perto do canto superior direito da interface.
- d. O EULA aparece. Role para baixo, selecione **Aceito para atualizações atuais e futuras** e selecione **Salvar**.

### Opções de atualização

Escolha uma das seguintes opções de atualização de firmware de armazenamento:

- [Use a IU do Controle de nuvem híbrida da NetApp para atualizar o firmware do storage](#)
- [Use a API de controle de nuvem híbrida da NetApp para atualizar o firmware de storage](#)

### Use a IU do Controle de nuvem híbrida da NetApp para atualizar o firmware do storage

Você pode usar a IU do Controle de nuvem híbrida da NetApp para atualizar o firmware dos nós de storage no cluster.

### O que você vai precisar

Se o nó de gerenciamento não estiver conectado à Internet, você "[Fez download do pacote de firmware de storage para clusters de storage do NetApp HCI](#)" terá o .



Para possíveis problemas durante a atualização dos clusters de storage usando o Controle de nuvem híbrida da NetApp e suas soluções alternativas, consulte este "[Artigo da KB](#)".



O processo de atualização leva aproximadamente 30 minutos por nó de storage. Se você estiver atualizando um cluster de storage Element para o firmware de storage mais recente que a versão 2,76, os nós de storage individuais só serão reiniciados durante a atualização se o novo firmware tiver sido gravado no nó.

### Passos

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
3. Selecione **Upgrade** perto do canto superior direito da interface.
4. Na página **Upgrades**, selecione **Storage**.



A guia **Storage** lista os clusters de armazenamento que fazem parte da sua instalação. Se um cluster estiver inacessível pelo Controle de nuvem híbrida da NetApp, ele não será exibido na página **Upgrades**. Se você tiver clusters executando o Element 12,0 ou posterior, verá a versão atual do pacote de firmware listada para esses clusters. Se os nós em um único cluster tiverem versões de firmware diferentes ou à medida que a atualização progride, você verá **Multiple** na coluna **Current firmware Bundle Version**. Você pode selecionar **Multiple** para navegar até a página **nodes** para comparar versões de firmware. Se todos os clusters estiverem executando versões do Element anteriores a 12,0, você não verá nenhuma informação sobre números de versão do pacote de firmware. Esta informação também está disponível na página **nodes**. "[Veja seu inventário](#)"Consulte .

Se o cluster estiver atualizado e/ou nenhum pacote de atualização estiver disponível, os separadores **Element** e **firmware Only** não serão apresentados. Essas guias também não são exibidas quando uma atualização está em andamento. Se a guia **Element** for exibida, mas não a guia **firmware Only**, nenhum pacote de firmware estará disponível.

5. Selecione a seta suspensa ao lado do cluster que você está atualizando.
6. Selecione **Procurar** para carregar o pacote de atualização que transferiu.
7. Aguarde até que o upload seja concluído. Uma barra de progresso mostra o status do upload.



O upload do arquivo será perdido se você navegar para longe da janela do navegador.

É apresentada uma mensagem no ecrã depois de o ficheiro ser carregado e validado com êxito. A validação pode demorar vários minutos. Se você navegar para longe da janela do navegador nesta fase, o upload do arquivo será preservado.

8. Selecione **firmware only** (apenas firmware) e selecione a partir das versões de atualização disponíveis.
9. Selecione **Begin Upgrade**.



O **Status do Upgrade** muda durante a atualização para refletir o status do processo. Ele também muda em resposta às ações que você toma, como pausar a atualização, ou se a atualização retornar um erro. [Alterações de status da atualização](#)Consulte .



Enquanto a atualização estiver em andamento, você pode sair da página e voltar a ela mais tarde para continuar monitorando o progresso. A página não atualiza dinamicamente o status e a versão atual se a linha do cluster for recolhida. A linha do cluster deve ser expandida para atualizar a tabela ou você pode atualizar a página.

Pode transferir registos após a conclusão da atualização.

#### Alterações de status da atualização

Aqui estão os diferentes estados que a coluna **Status da atualização** na IU mostra antes, durante e após o processo de atualização:

Estado de atualização	Descrição
Atualizado	O cluster foi atualizado para a versão mais recente do Element disponível ou o firmware foi atualizado para a versão mais recente.

Estado de atualização	Descrição
Não foi possível detectar	Esse status é exibido quando a API de serviço de armazenamento retorna um status de atualização que não está na lista enumerada de possíveis status de atualização.
Versões disponíveis	Versões mais recentes do Element e/ou firmware de storage estão disponíveis para atualização.
Em curso	A atualização está em andamento. Uma barra de progresso mostra o status da atualização. As mensagens na tela também mostram falhas no nível do nó e exibem a ID do nó de cada nó no cluster à medida que a atualização progride. Você pode monitorar o status de cada nó usando a IU do Element ou o plug-in do NetApp Element para a IU do vCenter Server.
Atualizar Pausando	Você pode optar por pausar a atualização. Dependendo do estado do processo de atualização, a operação de pausa pode ser bem-sucedida ou falhar. Você verá um prompt da interface do usuário solicitando que você confirme a operação de pausa. Para garantir que o cluster esteja em um local seguro antes de pausar uma atualização, pode levar até duas horas para que a operação de atualização seja completamente pausada. Para retomar a atualização, selecione <b>Resume</b> .
Em pausa	Fez uma pausa na atualização. Selecione <b>Resume</b> para retomar o processo.
Erro	Ocorreu um erro durante a atualização. Você pode baixar o log de erros e enviá-lo para o suporte da NetApp. Depois de resolver o erro, você pode retornar à página e selecionar <b>Resume</b> . Quando você retoma a atualização, a barra de progresso recua por alguns minutos enquanto o sistema executa a verificação de integridade e verifica o estado atual da atualização.

### O que acontece se uma atualização falhar usando o controle de nuvem híbrida da NetApp

Se uma unidade ou nó falhar durante uma atualização, a IU do Element mostrará falhas de cluster. O processo de atualização não avança para o nó seguinte e aguarda a resolução das falhas do cluster. A barra de progresso na IU mostra que a atualização está aguardando a resolução das falhas do cluster. Nesta fase, selecionar **Pausa** na IU não funcionará, porque a atualização aguarda que o cluster esteja saudável. Você precisará ativar o suporte da NetApp para ajudar na investigação de falha.

O controle de nuvem híbrida da NetApp tem um período de espera pré-definido de três horas, durante o qual um dos seguintes cenários pode acontecer:

- As falhas do cluster são resolvidas dentro da janela de três horas e a atualização é retomada. Você não precisa tomar nenhuma ação nesse cenário.
- O problema persiste após três horas e o status da atualização mostra **erro** com um banner vermelho. Você pode retomar a atualização selecionando **Resume** após o problema ser resolvido.

- O suporte da NetApp determinou que a atualização precisa ser temporariamente cancelada para tomar medidas corretivas antes da janela de três horas. O suporte usará a API para cancelar a atualização.



Abortar a atualização do cluster enquanto um nó está sendo atualizado pode resultar na remoção desgraciosa das unidades do nó. Se as unidades forem removidas sem graça, adicionar as unidades de volta durante uma atualização exigirá intervenção manual pelo suporte da NetApp. O nó pode estar demorando mais para fazer atualizações de firmware ou atividades de sincronização pós-atualização. Se o progresso da atualização parecer interrompido, entre em Contato com o suporte da NetApp para obter assistência.

## Use a API de controle de nuvem híbrida da NetApp para atualizar o firmware de storage

Você pode usar APIs para atualizar nós de storage em um cluster para a versão mais recente do software Element. Você pode usar uma ferramenta de automação de sua escolha para executar as APIs. O fluxo de trabalho da API documentado aqui usa a IU da API REST disponível no nó de gerenciamento como exemplo.

### Passos

1. Transfira o pacote de atualização de firmware de armazenamento mais recente para um dispositivo acessível ao nó de gestão; acesse ao "[Página do pacote de firmware de storage do software Element](#)" e transfira a imagem de firmware de armazenamento mais recente.
2. Carregue o pacote de atualização do firmware de armazenamento para o nó de gestão:
  - a. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
    - i. Introduza o nome de utilizador e a palavra-passe do cluster.
    - ii. Introduza a ID do cliente como `mnode-client`.
    - iii. Selecione **autorizar** para iniciar uma sessão.
    - iv. Feche a janela autorização.
  - c. Na IU da API REST, selecione **POST /packages**.
  - d. Selecione **Experimente**.
  - e. Selecione **Procurar** e selecione o pacote de atualização.
  - f. Selecione **execute** para iniciar o upload.
  - g. Na resposta, copie e salve o ID do ("id" pacote ) para uso em uma etapa posterior.
3. Verifique o status do upload.
    - a. Na IU da API REST, selecione **GET /packages/ id/status**.
    - b. Selecione **Experimente**.
    - c. Insira a ID do pacote de firmware que você copiou na etapa anterior em **id**.
    - d. Selecione **execute** para iniciar a solicitação de status.

A resposta indica `state` como `SUCCESS` quando concluída.

4. Localize o ID do ativo de instalação:

- a. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
- Introduza o nome de utilizador e a palavra-passe do cluster.
  - Introduza a ID do cliente como `mnode-client`.
  - Selecione **autorizar** para iniciar uma sessão.
  - Feche a janela autorização.
- c. Na IU da API REST, selecione **GET /installations**.
- d. Selecione **Experimente**.
- e. Selecione **Executar**.
- f. Na resposta, copie o ID do ativo de instalação (`id`).

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

- g. Na IU da API REST, selecione `*GET /installations/`
- h. Selecione **Experimente**.
- Cole o ID do ativo de instalação no campo `id`.
  - Selecione **Executar**.
- k. A partir da resposta, copie e salve o ID do cluster de armazenamento ("`id`") do cluster que pretende atualizar para uso em uma etapa posterior.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Execute a atualização do firmware de armazenamento:
- Abra a IU da API REST de storage no nó de gerenciamento:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
  - i. Introduza o nome de utilizador e a palavra-passe do cluster.
  - ii. Introduza a ID do cliente como `mnode-client`.
  - iii. Selecione **autorizar** para iniciar uma sessão.
  - iv. Feche a janela.
- c. Selecione **POST /Upgrades**.
- d. Selecione **Experimente**.
- e. Introduza a ID do pacote de atualização no campo Parameter (parâmetro).
- f. Introduza a ID do cluster de armazenamento no campo Parameter (parâmetro).
- g. Selecione **execute** para iniciar a atualização.

A resposta deve indicar o estado `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log"
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
```

```

"step": "ClusterPreStart",
"timestamp": "2020-04-21T22:10:57.057Z",
"failedHealthChecks": [
  {
    "checkID": 0,
    "name": "string",
    "displayName": "string",
    "passed": true,
    "kb": "string",
    "description": "string",
    "remedy": "string",
    "severity": "string",
    "data": {},
    "nodeID": 0
  }
],
"taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
"dateCompleted": "2020-04-21T22:10:57.057Z",
"dateCreated": "2020-04-21T22:10:57.057Z"
}

```

- a. Copie o ID de atualização ("upgradeId") que faz parte da resposta.
6. Verifique o progresso e os resultados da atualização:
- a. Selecione \*GET /Upgrades/
  - b. Selecione **Experimente**.
  - c. Insira o ID de atualização da etapa anterior em **upgradeId**.
  - d. Selecione **Executar**.
  - e. Siga um destes procedimentos se houver problemas ou requisitos especiais durante a atualização:

Opção	Passos
<p>Você precisa corrigir problemas de integridade do cluster devido a <code>failedHealthChecks</code> mensagem no corpo de resposta.</p>	<ol style="list-style-type: none"> <li>i. Vá para o artigo específico da KB listado para cada problema ou execute o recurso especificado.</li> <li>ii. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.</li> <li>iii. Depois de resolver problemas de cluster, reautentique se necessário e selecione <code>*put /Upgrades/</code></li> <li>iv. Selecione <b>Experimente</b>.</li> <li>v. Insira o ID de atualização da etapa anterior em <code>upgradedId</code>.</li> <li>vi. Introduza <code>"action": "resume"</code> o corpo do pedido. <div data-bbox="915 716 1487 898" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>{   "action": "resume" }</pre> </div> </li> <li>vii. Selecione <b>Executar</b>.</li> </ol>
<p>Você precisa pausar a atualização porque a janela de manutenção está fechando ou por outro motivo.</p>	<ol style="list-style-type: none"> <li>i. Reautentique se necessário e selecione <code>*put /Upgrades/</code></li> <li>ii. Selecione <b>Experimente</b>.</li> <li>iii. Insira o ID de atualização da etapa anterior em <code>upgradedId</code>.</li> <li>iv. Introduza <code>"action": "pause"</code> o corpo do pedido. <div data-bbox="915 1333 1487 1516" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>{   "action": "pause" }</pre> </div> </li> <li>v. Selecione <b>Executar</b>.</li> </ol>

f. Execute a API **GET /Upgrades/"upgradedId"** várias vezes, conforme necessário, até que o processo esteja concluído.

Durante a atualização, o `status` indica `running` se não foram encontrados erros. À medida que cada nó é atualizado, o `step` valor muda para `NodeFinished`.

A atualização foi concluída com êxito quando o `percent` valor é 100 e o `state` indica `finished`.

## Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Atualizar um nó de gerenciamento

Você pode atualizar seu nó de gerenciamento para o nó de gerenciamento 12,5 ou posterior a partir da versão 12,3.x ou posterior.

A atualização do sistema operacional de nós de gerenciamento não é mais necessária para atualizar o software Element no cluster de storage. Basta atualizar os serviços de gerenciamento para a versão mais recente para realizar atualizações de elementos usando o Controle de nuvem híbrida da NetApp. Siga o procedimento de atualização do nó de gerenciamento para o cenário se desejar atualizar o sistema operacional do nó de gerenciamento por outros motivos, como correção de segurança.



Se você precisar de informações sobre a atualização dos nós de gerenciamento 12,2 ou anteriores, consulte o ["Documentação de atualização do nó de gerenciamento do NetApp HCI 1,9"](#).

### Opções de atualização

Escolha uma das seguintes opções:

- [5 ou posterior a partir da versão 12,3.x ou posterior](#)
- [Reconfigure a autenticação usando a API REST do nó de gerenciamento](#)

Escolha esta opção se você tiver **sequencialmente** atualizado (1) a versão dos serviços de gerenciamento e (2) a versão de armazenamento de elementos e quiser **manter** o nó de gerenciamento existente:



Se você não atualizar sequencialmente seus serviços de gerenciamento seguidos pelo armazenamento de elementos, não poderá reconfigurar a reautenticação usando este procedimento. Em vez disso, siga o procedimento de atualização apropriado.

## Atualize um nó de gerenciamento para a versão 12,5 ou posterior a partir da versão 12,3.x ou posterior

Você pode fazer uma atualização no local do nó de gerenciamento da versão 12,3.x ou posterior para a versão 12,5 ou posterior sem precisar provisionar uma nova máquina virtual de nó de gerenciamento.



O nó de gerenciamento do Element 12,5 ou posterior é uma atualização opcional. Não é necessário para implantações existentes.

### O que você vai precisar

- A RAM da VM do nó de gerenciamento é 24GB.
- O nó de gerenciamento que você pretende atualizar é a versão 12,0 e usa a rede IPv4. O nó de gerenciamento versão 12,5 ou posterior não suporta IPv6.



Para verificar a versão do nó de gerenciamento, faça login no nó de gerenciamento e veja o número da versão do elemento no banner de login.

- Você atualizou seu pacote de serviços de gerenciamento para a versão mais recente usando o controle de nuvem híbrida da NetApp. Você pode acessar o controle de nuvem híbrida da NetApp a partir do seguinte IP: `https://<ManagementNodeIP>`
- Se você estiver atualizando seu nó de gerenciamento para a versão 12,5 ou posterior, precisará dos serviços de gerenciamento 2.21.61 ou posterior para continuar.
- Você configurou um adaptador de rede adicional (se necessário) usando as instruções do ["Configurando uma NIC de armazenamento adicional"](#).



Os volumes persistentes podem exigir um adaptador de rede adicional se o eth0 não puder ser roteado para o SVIP. Configure um novo adaptador de rede na rede de armazenamento iSCSI para permitir a configuração de volumes persistentes.

- Os nós de storage estão executando o elemento 12,3.x ou posterior.

## Passos

1. Faça login na máquina virtual do nó de gerenciamento usando SSH ou acesso ao console.
2. Faça o download do ["Nó de gestão ISO"](#) software for Element do site de suporte da NetApp para a máquina virtual do nó de gerenciamento.



O nome do ISO é semelhante `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Verifique a integridade do download executando o md5sum no arquivo baixado e compare a saída com o que está disponível no site de suporte da NetApp para o software Element, como no exemplo a seguir:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Monte a imagem ISO do nó de gerenciamento e copie o conteúdo para o sistema de arquivos usando os seguintes comandos:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Mude para o diretório inicial e desmonte o arquivo ISO de /mnt:

```
sudo umount /mnt
```

6. Exclua o ISO para economizar espaço no nó de gerenciamento:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-  
XX.X.X.XXXX.iso
```

7. No nó de gerenciamento que você está atualizando, execute o seguinte comando para atualizar a versão do SO do nó de gerenciamento. O script retém todos os arquivos de configuração necessários após a atualização, como o coletor Active IQ e as configurações de proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

O nó de gerenciamento reinicializa com um novo sistema operacional após a conclusão do processo de atualização.



Depois de executar o comando sudo descrito nesta etapa, a sessão SSH é morta. O acesso ao console é necessário para monitoramento contínuo. Se não houver acesso ao console disponível ao executar a atualização, tente novamente o login SSH e verifique a conectividade após 15 a 30 minutos. Depois de fazer login, você pode confirmar a nova versão do sistema operacional no banner SSH que indica que a atualização foi bem-sucedida.

8. No nó de gerenciamento, execute o `redploy-mnode` script para reter as configurações anteriores dos serviços de gerenciamento:



O script retém a configuração anterior dos serviços de gerenciamento, incluindo a configuração do serviço coletor Active IQ, controladores (vCenters) ou proxy, dependendo de suas configurações.

```
sudo /sf/packages/mnode/redploy-mnode -mu <mnode user>
```



Se você já tinha desabilitado a funcionalidade SSH no nó de gerenciamento, você precisa ["Desative o SSH novamente"](#) no nó de gerenciamento recuperado. O recurso SSH que fornece ["Acesso à sessão do túnel de suporte remoto \(RST\) do suporte da NetApp"](#) está habilitado no nó de gerenciamento por padrão.

## Reconfigure a autenticação usando a API REST do nó de gerenciamento

Você pode manter seu nó de gerenciamento existente se tiver atualizado sequencialmente (1) serviços de gerenciamento e (2) storage de elementos. Se você seguiu uma ordem de atualização diferente, consulte os procedimentos para atualizações de nós de gerenciamento no local.

### Antes de começar

- Você atualizou seus serviços de gerenciamento para 2.20.69 ou posterior.
- Seu cluster de storage está executando o Element 12,3 ou posterior.
- Você atualizou seus serviços de gerenciamento sequencialmente, seguindo a atualização do storage Element. Não é possível reconfigurar a autenticação utilizando este procedimento, a menos que tenha

concluído atualizações na sequência descrita.

## Passos

1. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/mnode
```

2. Selecione **autorizar** e preencha o seguinte:
  - a. Introduza o nome de utilizador e a palavra-passe do cluster.
  - b. Introduza a ID do cliente como `mnode-client` se o valor ainda não estivesse preenchido.
  - c. Selecione **autorizar** para iniciar uma sessão.
3. Na IU da API REST, selecione **POST /services/reconfigure-auth**.
4. Selecione **Experimente**.
5. Para o parâmetro **load\_images**, `true` selecione .
6. Selecione **Executar**.

O corpo de resposta indica que a reconfiguração foi bem-sucedida.

## Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Atualize o plug-in Element para o vCenter Server

Para ambientes vSphere existentes com um plug-in NetApp Element registrado para VMware vCenter Server, você pode atualizar o Registro do plug-in depois de atualizar o pacote de serviços de gerenciamento que contém o serviço do plug-in.

Você pode atualizar o Registro do plug-in no vCenter Server Virtual Appliance (vCSA) ou Windows usando o utilitário de Registro. Você deve alterar seu Registro para o vCenter Plug-in em cada vCenter Server onde você precisa usar o plug-in.



Os serviços de gerenciamento 2.22.7 incluem o plug-in Element para vCenter Server 5,0 que contém o plug-in remoto. Se você usar o plug-in Element, você deve atualizar para os serviços de gerenciamento 2.22.7 ou posterior para cumprir com a diretiva VMware que remove o suporte para plug-ins locais. ["Saiba mais"](#).

### Plug-in Element para vCenter 5,0 e posterior

Este procedimento de atualização abrange os seguintes cenários de atualização:

- Você está atualizando para o Element Plug-in para vCenter Server 5,4, 5,3, 5,2, 5,1 ou 5,0.
- Você está atualizando para um 8,0 ou 7,0 HTML5 vSphere Web Client.



O plug-in Element para vCenter 5,0 ou posterior não é compatível com o vCenter Server 6,7 e 6,5.



Quando você atualiza do Element Plug-in para vCenter Server 4.x para 5.x, os clusters já configurados com o plug-in são perdidos porque os dados não podem ser copiados de uma instância do vCenter para um plug-in remoto. Você deve adicionar novamente os clusters ao plug-in remoto. Essa é uma atividade única ao atualizar de um plug-in local para um plug-in remoto.

### Plug-in Element para vCenter 4,10 e anterior

Este procedimento de atualização abrange os seguintes cenários de atualização:

- Você está atualizando para o Element Plug-in para vCenter Server 4,10, 4,9, 4,8, 4,7, 4,6, 4,5 ou 4,4.
- Você está atualizando para um vSphere Web Client 7,0, 6,7 ou 6,5 HTML5.

- O plug-in não é compatível com o VMware vCenter Server 8,0 para Element Plug-in para VMware vCenter Server 4.x.
- O plug-in não é compatível com o VMware vCenter Server 6,5 para plug-in Element para VMware vCenter Server 4,6, 4,7 e 4,8.

- Você está atualizando para um 6,7 Flash vSphere Web Client.



O plug-in não é compatível com a versão 6,7 U2 build 13007421 do HTML5 vSphere Web Client e outras versões 6,7 U2 lançadas antes da atualização 2a (compilação 13643870). Para obter mais informações sobre as versões do vSphere suportadas, consulte as notas de versão "[sua versão do plug-in](#)" do .

### O que você vai precisar

- **Admin Privileges:** Você tem o vCenter Administrator Role Privileges para instalar um plug-in.
- **Atualizações do vSphere:** Você executou todas as atualizações necessárias do vCenter antes de atualizar o plug-in do NetApp Element para o vCenter Server. Este procedimento pressupõe que as atualizações do vCenter já foram concluídas.
- **vCenter Server:** O plug-in do vCenter versão 4.x ou 5.x está registrado em um vCenter Server. No utilitário de Registro ([https://\[management node IP\]:9443](https://[management node IP]:9443)), selecione **Status do Registro**, preencha os campos necessários e selecione **verificar status** para verificar se o plug-in do vCenter já está registrado e o número da versão da instalação atual.
- **Atualizações de serviços de gerenciamento:** Você atualizou o seu "[pacote de serviços de gerenciamento](#)" para a versão mais recente. As atualizações do plug-in do vCenter são distribuídas usando atualizações de serviços de gerenciamento que são lançadas fora das principais versões de

produtos para o NetApp HCI.

- **Atualizações de nó de gerenciamento:**

**Plug-in Element para vCenter 5,0 e posterior**

Você está executando um nó de gerenciamento que foi "atualizado" para a versão 12,3.x ou posterior.

**Plug-in Element para vCenter 4,10 e anterior**

Você está executando um nó de gerenciamento que foi "atualizado" para a versão 11,3 ou posterior. O vCenter Plug-in 4,4 ou posterior requer um nó de gerenciamento 11,3 ou posterior com uma arquitetura modular que forneça serviços individuais. Seu nó de gerenciamento deve ser ligado com seu endereço IP ou endereço DHCP configurado.

- \* Atualizações de armazenamento Element\*:

- A partir do plug-in do Element vCenter 5,0, você tem um cluster executando o software NetApp Element 12,3.x ou posterior.

- Para o plug-in Element vCenter 4,10 ou anterior, você tem um cluster executando o software NetApp Element 11,3 ou posterior.

- **VSphere Web Client:** Você fez logout do vSphere Web Client antes de iniciar qualquer atualização do plug-in. O cliente web não reconhecerá atualizações feitas durante este processo para o plug-in se você não terminar sessão.

## Passos

1. Insira o endereço IP do seu nó de gerenciamento em um navegador, incluindo a porta TCP para Registro: `https://[management node IP]:9443` A IU do utilitário de Registro será aberta para a página **Gerenciar credenciais do serviço QoSSIOC** do plug-in.

QoSSIOC Management

- Manage Credentials
- Restart QoSSIOC Service

### Manage QoSSIOC Service Credentials

**Old Password**   
Current password is required

**New Password**   
Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like #!@:()~!@#%^&\*~

**Confirm Password**   
New and confirm passwords must match

Contact NetApp Support at <http://mysupport.netapp.com>

2. Selezione **Registo do plug-in do vCenter.**

## Plug-in Element para vCenter 5,0 e posterior

A página Registro do plug-in do vCenter é exibida:

**NetApp** Element Plug-in for vCenter Server Management Node

GoSSIOC Service Management vCenter Plug-in Registration

**Manage vCenter Plug-in**

- Register Plug-in
- Update Plug-in
- Unregister Plug-in
- Registration Status

### vCenter Plug-in - Registration

Register version 5.0.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration.

**vCenter Address**   
Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

**vCenter User Name**   
Ensure this user is a vCenter user that has administrative privileges for registration.

**vCenter Password**   
The password for the vCenter user name entered.

**Customize URL**  
Select to customize the Zip file URL.

**Plug-in Zip URL**   
URL of XML initialization file

**REGISTER**

Contact NetApp Support at <http://mysupport.netapp.com>

## Plug-in Element para vCenter 4,10 e anterior

A página Registro do plug-in do vCenter é exibida:

Manage vCenter Plug-in

- Register Plug-in
- Update Plug-in
- Unregister Plug-in
- Registration Status

### vCenter Plug-in - Registration

Register version [ ] of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration.

**vCenter Address**   
Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

**vCenter User Name**   
Ensure this user is a vCenter user that has administrative privileges for registration.

**vCenter Password**   
The password for the vCenter user name entered.

Customize URL  
Select to customize the Zip file URL.

**Plug-in Zip URL**   
URL of XML initialization file.

**REGISTER**

Contact NetApp Support at <http://mysupport.netapp.com>

3. Em **Manage vCenter Plug-in**, selecione **Update Plug-in**.

4. Confirme ou atualize as seguintes informações:

- O endereço IPv4 ou o FQDN do serviço vCenter no qual você registrará seu plug-in.
- O nome de usuário do vCenter Administrator.



O nome de usuário e as credenciais de senha inseridas devem ser para um usuário com o vCenter Administrator role Privileges.

- A senha do vCenter Administrator.
- (Para servidores internos ou dark sites) dependendo do plug-in Element para a versão vCenter, um URL personalizado para o arquivo JSON plug-in ou ZIP plug-in:

#### Plug-in Element para vCenter 5,0 e posterior

Um URL personalizado para o arquivo JSON plug-in.



Você pode selecionar **URL personalizado** para personalizar o URL se estiver usando um servidor HTTP ou HTTPS (site escuro) ou tiver modificado o nome do arquivo JSON ou as configurações de rede. Para obter etapas de configuração adicionais se você pretende personalizar um URL, consulte a documentação do Element Plug-in para vCenter Server sobre como modificar propriedades do vCenter para um servidor HTTP interno (dark site).

#### Plug-in Element para vCenter 4,10 e anterior

Um URL personalizado para o ZIP do plug-in.



Você pode selecionar **URL personalizado** para personalizar o URL se estiver usando um servidor HTTP ou HTTPS (site escuro) ou tiver modificado o nome do arquivo ZIP ou as configurações de rede. Para obter etapas de configuração adicionais se você pretende personalizar um URL, consulte a documentação do Element Plug-in para vCenter Server sobre como modificar propriedades do vCenter para um servidor HTTP interno (dark site).

#### 5. Selecione **Atualizar**.

Um banner aparece na IU do utilitário de Registro quando o Registro é bem-sucedido.

#### 6. Faça login no vSphere Web Client como um vCenter Administrator. Se você já estiver logado no vSphere Web Client, primeiro deverá fazer logout, aguardar dois a três minutos e, em seguida, fazer login novamente.



Essa ação cria um novo banco de dados e conclui a instalação no vSphere Web Client.

#### 7. No vSphere Web Client, procure as seguintes tarefas concluídas no monitor de tarefas para garantir que a instalação foi concluída: Download plug-in E Deploy plug-in.

#### 8. Verifique se os pontos de extensão do plug-in aparecem na guia **Atalhos** do vSphere Web Client e no painel lateral.

#### Plug-in Element para vCenter 5,0 e posterior

O ponto de extensão do plug-in remoto do NetApp Element é exibido:

—

#### Plug-in Element para vCenter 4,10 e anterior

Os pontos de extensão Configuração e Gerenciamento do NetApp Element são exibidos:

—

Se os ícones do plug-in do vCenter não estiverem visíveis, "[Plug-in Element para vCenter Server](#)" consulte a documentação sobre solução de problemas do plug-in.



Depois de atualizar para o plug-in do NetApp Element para o vCenter Server 4,8 ou posterior com o VMware vCenter Server 6.7U1, se os clusters de armazenamento não estiverem listados ou um erro de servidor aparecer nas seções **clusters** e **Configurações de QoSSIOC** da Configuração do NetApp Element, consulte "[Plug-in Element para vCenter Server](#)" a documentação sobre a solução de problemas desses erros.

9. Verifique a alteração de versão na guia **sobre** no ponto de extensão **Configuração do NetApp Element** do plug-in.

Você deve ver os seguintes detalhes de versão ou detalhes de uma versão mais recente:

```
NetApp Element Plug-in Version: 5.4
NetApp Element Plug-in Build Number: 1
```



O plug-in do vCenter contém conteúdo de ajuda on-line. Para garantir que a Ajuda contenha o conteúdo mais recente, limpe o cache do navegador depois de atualizar o plug-in.

### Encontre mais informações

- "[Plug-in do NetApp Element para vCenter Server](#)"
- "[Página de recursos do NetApp HCI](#)"

### Execute verificações de integridade do nó de computação antes de atualizar o firmware da computação

É necessário executar verificações de integridade antes de atualizar o firmware da computação para garantir que todos os nós de computação no cluster estejam prontos para ser atualizados. As verificações de integridade do nó de computação só podem ser executadas em clusters de computação de um ou mais nós de computação NetApp HCI gerenciados.

#### O que você vai precisar

- **Serviços de gerenciamento:** Você atualizou para o pacote de serviços de gerenciamento mais recente (2,11 ou posterior).
- **Nó de gerenciamento:** Você está executando o nó de gerenciamento 11,3 ou posterior.
- **Software Element:** Seu cluster de armazenamento está executando o software NetApp Element 11,3 ou posterior.
- **Contrato de Licença de Usuário final (EULA):** Começando com os serviços de gerenciamento 2.20.69, você deve aceitar e salvar o EULA antes de usar a IU ou API do Controle de nuvem híbrida da NetApp para executar verificações de integridade do nó de computação:
  - a. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

- b. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
- c. Selecione **Upgrade** perto do canto superior direito da interface.
- d. O EULA aparece. Role para baixo, selecione **Aceito para atualizações atuais e futuras** e selecione **Salvar**.

### Opções de verificação de integridade

Você pode executar verificações de integridade usando a IU do Controle de nuvem híbrida da NetApp ou a API de controle de nuvem híbrida da NetApp:

- [Use o Controle de nuvem híbrida da NetApp para executar verificações de integridade dos nós de computação antes de atualizar o firmware](#) (Método preferido)
- [Use a API para executar verificações de integridade do nó de computação antes de atualizar o firmware](#)

Saiba mais sobre as verificações de integridade dos nós de computação executadas pelo serviço:

- [Verificações de integridade do nó de computação feitas pelo serviço](#)

### Use o Controle de nuvem híbrida da NetApp para executar verificações de integridade dos nós de computação antes de atualizar o firmware

Com o Controle de nuvem híbrida da NetApp, você pode verificar se um nó de computação está pronto para uma atualização de firmware.



Se você tiver várias configurações de cluster de storage de dois nós, cada uma no seu próprio vCenter, as verificações de integridade dos nós de testemunha podem não ser relatadas com precisão. Portanto, quando você estiver pronto para atualizar os hosts ESXi, você só deve encerrar o nó de testemunha no host ESXi que está sendo atualizado. Você deve garantir que você sempre tenha um nó de testemunha em execução em sua instalação do NetApp HCI desligando os nós de testemunha de forma alternativa.

### Passos

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>/hcc
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
3. Selecione **Upgrade** perto do canto superior direito da interface.
4. Na página **Upgrades**, selecione a guia **Compute firmware**.
5. Selecione a verificação de integridade  do cluster que deseja verificar se há disponibilidade de atualização.
6. Na página **Compute Health Check**, selecione **Run Health Check**.

7. Se houver problemas, a página fornece um relatório. Faça o seguinte:
  - a. Vá para o artigo específico da KB listado para cada problema ou execute o recurso especificado.
  - b. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.
  - c. Depois de resolver problemas de cluster, selecione **Re-Run Health Check**.

Depois que a verificação de integridade for concluída sem erros, os nós de computação no cluster estarão prontos para atualização. ["Atualize o firmware do nó de computação"](#) Consulte para continuar.

### Use a API para executar verificações de integridade do nó de computação antes de atualizar o firmware

Você pode usar a API REST para verificar se os nós de computação em um cluster estão prontos para ser atualizados. A verificação de integridade verifica se não há obstáculos para atualizar, como problemas de host ESXi ou outros problemas do vSphere. Você precisará executar verificações de integridade dos nós de computação para cada cluster de computação no seu ambiente.

#### Passos

1. Localize a ID do controlador e a ID do cluster:
  - a. Abra a IU da API REST do serviço de inventário no nó de gerenciamento:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
  - i. Introduza o nome de utilizador e a palavra-passe do cluster.
  - ii. Introduza a ID do cliente como `mnode-client` se o valor ainda não estivesse preenchido.
  - iii. Selecione **autorizar** para iniciar uma sessão.
- c. Na IU da API REST, selecione **GET /installations**.
- d. Selecione **Experimente**.
- e. Selecione **Executar**.
- f. A partir do corpo de resposta do código 200, copie o "id" para a instalação que pretende utilizar para verificações de integridade.
- g. Na IU da API REST, selecione `*GET /installations/`
- h. Selecione **Experimente**.
  - i. Introduza a ID de instalação.
- j. Selecione **Executar**.
- k. A partir do corpo de resposta do código 200, copie os IDs para cada um dos seguintes itens:
  - i. O ID do cluster ("`clusterID`")
  - ii. Um ID do controlador ("`controllerId`")

```

{
  "_links": {
    "collection":
    "https://10.117.187.199/inventory/1/installations",
    "self":
    "https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-
    412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-
          4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ]
    },
  },
}

```

2. Execute verificações de integridade nos nós de computação no cluster:

- a. Abra a IU da API REST do serviço de computação no nó de gerenciamento:

```
https://<ManagementNodeIP>/vcenter/1/
```

- b. Selecione **autorizar** e preencha o seguinte:

- i. Introduza o nome de utilizador e a palavra-passe do cluster.
- ii. Introduza a ID do cliente como `mnode-client` se o valor ainda não estivesse preenchido.
- iii. Selecione **autorizar** para iniciar uma sessão.

- c. Selecione **POST /compute/ CONTROLLER\_ID/health-checks**.

- d. Selecione **Experimente**.

- e. Digite o "controllerId" que você copiou da etapa anterior no campo de parâmetro **Controller\_ID**.

- f. Na carga útil, insira o "clusterId" que você copiou da etapa anterior como o "cluster" valor e

remova o "nodes" parâmetro.

```
{
  "cluster": "domain-1"
}
```

g. Selecione **execute** para executar uma verificação de integridade no cluster.

A resposta do código 200 fornece "resourceLink" um URL com o ID da tarefa anexado que é necessário para confirmar os resultados da verificação de integridade.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This
is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

a. Copie a parte da ID da tarefa "resourceLink" do URL para verificar o resultado da tarefa.

3. Verifique o resultado das verificações de integridade:

a. Retorno à IU da API REST do serviço de computação no nó de gerenciamento:

```
https://<ManagementNodeIP>/vcenter/1/
```

b. Selecione **GET /compute/Tasks/(tarefa\_id)**.

c. Selecione **Experimente**.

d. Digite a parte da ID da tarefa "resourceLink" do URL da resposta do código **POST /compute/CONTROLLER\_ID/health-checks** 200 no `task_id` campo parâmetro.

e. Selecione **Executar**.

f. Se o `status` retornado indicar que houve problemas em relação à integridade do nó de computação, faça o seguinte:

i. Vá para o artigo específico da KB (`KbLink`) listado para cada problema ou execute a solução especificada.

ii. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.

iii. Depois de resolver problemas de cluster, execute **POST /compute/CONTROLLER\_ID/Health-checks** novamente (consulte a etapa 2).

Se as verificações de integridade forem concluídas sem problemas, o código de resposta 200 indica um resultado bem-sucedido.

## Verificações de integridade do nó de computação feitas pelo serviço

As verificações de integridade da computação, sejam elas realizadas pelo Controle de nuvem híbrida ou pelos métodos de API da NetApp, fazem as seguintes verificações por nó. Dependendo do seu ambiente, algumas dessas verificações podem ser ignoradas. Você deve executar novamente as verificações de integridade depois de resolver quaisquer problemas detetados.

Verifique a descrição	Nó/cluster	Ação necessária para resolver	artigo da base de conhecimento com procedimento
O DRS está ativado e totalmente automatizado?	Cluster	Ative o DRS e certifique-se de que ele esteja totalmente automatizado.	<a href="#">"Veja este KB"</a> . OBSERVAÇÃO: Se você tiver o licenciamento padrão, coloque o host ESXi no modo de manutenção e ignore este aviso de falha de verificação de integridade.
O DPM está desativado no vSphere?	Cluster	Desligue o Gerenciamento de Energia distribuída.	<a href="#">"Veja este KB"</a> .
O controle de admissão de HA está desativado no vSphere?	Cluster	Desligue o controle de admissão HA.	<a href="#">"Veja este KB"</a> .
O FT está habilitado para uma VM em um host no cluster?	Nó	Suspenda a tolerância a falhas em qualquer máquina virtual afetada.	<a href="#">"Veja este KB"</a> .
Há alarmes críticos no vCenter para o cluster?	Cluster	Inicie o vSphere e resolva e/ou confirme quaisquer alertas antes de continuar.	Não é necessário nenhum KB para resolver o problema.
Existem alertas informativos genéricos/globais no vCenter?	Cluster	Inicie o vSphere e resolva e/ou confirme quaisquer alertas antes de continuar.	Não é necessário nenhum KB para resolver o problema.
Os serviços de gestão estão atualizados?	Sistema HCI	É necessário atualizar os serviços de gerenciamento antes de executar uma atualização ou verificações de integridade de pré-atualização.	Não é necessário nenhum KB para resolver o problema. Consulte <a href="#">"este artigo"</a> para obter mais informações.
Há erros no nó ESXi atual no vSphere?	Nó	Inicie o vSphere e resolva e/ou confirme quaisquer alertas antes de continuar.	Não é necessário nenhum KB para resolver o problema.
A Mídia virtual é montada em uma VM em um host no cluster?	Nó	Desmonte todos os discos de Mídia virtual (CD/DVD/floppy) das VMs.	Não é necessário nenhum KB para resolver o problema.

Verifique a descrição	Nó/cluster	Ação necessária para resolver	artigo da base de conhecimento com procedimento
A versão do BMC é a versão mínima necessária que tem suporte para o Redfish?	Nó	Atualize manualmente o firmware do BMC.	Não é necessário nenhum KB para resolver o problema.
O host ESXi está ativo e em execução?	Nó	Inicie seu host ESXi.	Não é necessário nenhum KB para resolver o problema.
As máquinas virtuais residem no armazenamento ESXi local?	Nó/VM	Remova ou migre o armazenamento local anexado a máquinas virtuais.	Não é necessário nenhum KB para resolver o problema.
O BMC está funcionando?	Nó	Ligue o seu BMC e certifique-se de que está ligado a uma rede que este nó de gestão pode alcançar.	Não é necessário nenhum KB para resolver o problema.
Há host(s) ESXi parceiro(s) disponível(s)?	Nó	Disponibilize um ou mais host(s) ESXi no cluster (não no modo de manutenção) para migrar máquinas virtuais.	Não é necessário nenhum KB para resolver o problema.
Você consegue se conectar com o BMC através do protocolo IPMI?	Nó	Ative o protocolo IPMI no controlador de gerenciamento de placa base (BMC).	Não é necessário nenhum KB para resolver o problema.
O host ESXi está mapeado corretamente para o host de hardware (BMC)?	Nó	O host ESXi não é mapeado corretamente para o controlador de gerenciamento da placa base (BMC). Corrija o mapeamento entre o host ESXi e o host de hardware.	Não é necessário nenhum KB para resolver o problema. Consulte <a href="#">"este artigo"</a> para obter mais informações.
Qual é o status dos nós de testemunha no cluster? Nenhum dos nós de testemunhas identificados está funcionando.	Nó	Um nó de testemunha não está sendo executado em um host ESXi alternativo. Ligue o nó testemunha em um host ESXi alternativo e execute novamente a verificação de integridade. <b>Um nó de testemunha deve estar em execução na instalação do HCI em todos os momentos.</b>	<a href="#">"Veja este KB"</a>

Verifique a descrição	Nó/cluster	Ação necessária para resolver	artigo da base de conhecimento com procedimento
Qual é o status dos nós de testemunha no cluster? O nó testemunha está ativo e em execução neste host ESXi e o nó testemunha alternativo não está ativo e funcionando.	Nó	Um nó de testemunha não está sendo executado em um host ESXi alternativo. Ligue o nó testemunha em um host ESXi alternativo. Quando estiver pronto para atualizar este host ESXi, encerre o nó testemunha em execução neste host ESXi e execute novamente a verificação de integridade. <b>Um nó de testemunha deve estar em execução na instalação do HCI em todos os momentos.</b>	<a href="#">"Veja este KB"</a>
Qual é o status dos nós de testemunha no cluster? O nó testemunha está ativo e em execução neste host ESXi e o nó alternativo está ativo, mas está em execução no mesmo host ESXi.	Nó	Ambos os nós de testemunha estão sendo executados neste host ESXi. Realocar um nó de testemunha para um host ESXi alternativo. Quando estiver pronto para atualizar este host ESXi, encerre o nó de testemunha que permanece neste host ESXi e execute novamente a verificação de integridade. <b>Um nó de testemunha deve estar em execução na instalação do HCI em todos os momentos.</b>	<a href="#">"Veja este KB"</a>
Qual é o status dos nós de testemunha no cluster? O nó testemunha está ativo e em execução neste host ESXi e o nó testemunha alternativo está ativo e em execução em outro host ESXi.	Nó	Um nó de testemunha está sendo executado localmente neste host ESXi. Quando estiver pronto para atualizar este host ESXi, encerre o nó testemunha somente neste host ESXi e execute novamente a verificação de integridade. <b>Um nó de testemunha deve estar em execução na instalação do HCI em todos os momentos.</b>	<a href="#">"Veja este KB"</a>

## Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Atualizar drivers de nós de computação

Para qualquer nó de computação da série H, é possível atualizar os drivers usados nos nós usando o VMware Update Manager.

### O que você vai precisar

Consulte a matriz de firmware e driver do hardware em ["Versões de firmware e driver ESXi compatíveis"](#).

### Sobre esta tarefa

Execute apenas uma dessas operações de atualização de cada vez.

Você deve verificar a versão atual do driver ESXi antes de tentar atualizar o firmware de computação. Se o driver estiver desatualizado, atualize o driver primeiro. Em seguida, atualize o firmware de computação para seus nós de computação.

### Passos

1. Navegue até a ["Downloads de software do NetApp HCI"](#) página e selecione o link de download para a versão correta do NetApp HCI.
2. Selecione **ESXI\_drivers** na lista suspensa.
3. Aceite o Contrato de Licença de Utilizador final.
4. Baixe o pacote de driver para o tipo de nó e a versão ESXi.
5. Extraia o pacote de drivers baixado no computador local.



O pacote de driver do NetApp inclui um ou mais arquivos ZIP do pacote off-line da VMware; não extraia esses arquivos ZIP.

6. Vá para **VMware Update Manager** no VMware vCenter.
7. Importe o arquivo de pacote off-line do driver para os nós de computação para o **Repositório de patches**.

Para VMware ESXi 6.x e 7,0 para 7,0 U3, execute as seguintes etapas para importar o arquivo de pacote offline do driver:

- a. Selecione a guia **atualizações**.
  - b. SELECIONE **UPLOAD DO ARQUIVO**.
  - c. Navegue até o pacote off-line que foi baixado anteriormente e selecione **IMPORT**.
8. Crie uma nova linha de base de host para o nó de computação.
  9. Escolha **Host Extension** para Nome e tipo e selecione todos os pacotes de driver importados a serem incluídos na nova linha de base.
  10. No menu **Host and clusters** no vCenter, selecione o cluster com os nós de computação que deseja atualizar e navegue até a guia **Update Manager**.
  11. Selecione **Remediate** e selecione a linha de base do host recém-criada. Certifique-se de que os controladores incluídos na linha de base estão selecionados.

12. Prossiga pelo assistente até a opção **Opções de correção do host** e certifique-se de que a opção **não alterar o estado de energia da VM** esteja selecionada para manter as máquinas virtuais on-line durante a atualização do driver.



Se o VMware Distributed Resource Scheduler (DRS) estiver habilitado no cluster (esse é o padrão nas instalações do NetApp HCI), as máquinas virtuais serão migradas automaticamente para outros nós no cluster.

13. Avance para a página **Pronto para concluir** no assistente e selecione **concluir**.

Os drivers de todos os nós de computação no cluster são atualizados um nó de cada vez, enquanto as máquinas virtuais permanecem online.

### Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

### Atualizar o firmware do nó de computação

Para nós de computação da série H, você pode atualizar o firmware para componentes de hardware, como BMC, BIOS e NIC. Para atualizar o firmware do nó de computação, você pode usar a IU do Controle de nuvem híbrida da NetApp, a API REST, uma unidade USB com a imagem de firmware mais recente ou a IU do BMC.

Após a atualização, o nó de computação inicializa no ESXi e funciona como antes, mantendo a configuração.

### O que você vai precisar

- **Compute drivers:** Você atualizou seus drivers de nó de computação. Se os drivers de nó de computação não forem compatíveis com o novo firmware, a atualização não será iniciada. Consulte o ["Ferramenta de Matriz de interoperabilidade \(IMT\)"](#) para obter informações sobre compatibilidade de driver e firmware e consulte o mais recente ["notas de versão do firmware do nó de computação"](#) para obter informações importantes sobre firmware e driver de última geração.
- **Admin Privileges:** Você tem permissões de administrador de cluster e administrador do BMC para executar a atualização.
- **Portas do sistema:** Se você estiver usando o Controle de nuvem híbrida da NetApp para atualizações, você garantiu que as portas necessárias estejam abertas. Consulte ["Portas de rede"](#) para obter mais informações.
- **Versões mínimas de BMC e BIOS:** O nó que você pretende atualizar usando o Controle de nuvem híbrida da NetApp atende aos seguintes requisitos mínimos:

Modelo	Versão mínima do BMC	Versão mínima do BIOS
H300E/H500E/H700E	6.84.00	NA2.1
H410C	Todas as versões suportadas (sem necessidade de atualização)	Todas as versões suportadas (sem necessidade de atualização)
H610C	3.96.07	3B01
H615C	4.68.07	3B08.CO



Os nós de computação do H615C devem atualizar o firmware do BMC para a versão 4,68 usando o ["pacote de firmware de computação 2,27"](#) para permitir que o Controle de nuvem híbrida da NetApp execute futuras atualizações de firmware.



Para obter uma matriz completa de firmware e firmware de driver para seu hardware, ["Versões de firmware e driver ESXi compatíveis"](#) consulte .

- **Ordem de inicialização do BIOS:** Altere manualmente a ordem de inicialização na configuração do BIOS para cada nó para garantir USB CD/DVD que apareça na lista de inicialização. Consulte este ["artigo"](#) documento para obter mais informações.
- **Credenciais do BMC:** Atualize as credenciais que o Controle de nuvem híbrida da NetApp usa para se conectar ao nó de computação BMC. Isso pode ser feito usando o controle de nuvem híbrida da NetApp ["UI"](#) ou ["API"](#) . A atualização das informações do BMC antes da atualização atualiza o inventário e garante que os serviços de nós de gerenciamento estejam cientes de todos os parâmetros de hardware necessários para concluir a atualização.
- \* Mídia anexada\*: Desconecte qualquer USB físico ou ISO antes de iniciar uma atualização de nó de computação.
- \* Console KVM ESXi\*: Feche todas as sessões Open Serial-over-laN (sol) e sessões KVM ativas na IU do BMC antes de iniciar uma atualização do nó de computação.
- **Requisitos de nó testemunha:** Em clusters de armazenamento de dois e três nós, um ["Witness Node"](#) deve estar sempre em execução na instalação do NetApp HCI.
- **Verificação de integridade do nó de computação:** Você verificou que o nó está pronto para ser atualizado. ["Execute verificações de integridade do nó de computação antes de atualizar o firmware da computação"](#) Consulte .
- **Contrato de Licença de Usuário final (EULA):** Começando com os serviços de gerenciamento 2.20.69, você deve aceitar e salvar o EULA antes de usar a interface de usuário ou API do NetApp Hybrid Cloud Control para atualizar o firmware do nó de computação:
  - a. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

- b. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.
- c. Selecione **Upgrade** perto do canto superior direito da interface.
- d. O EULA aparece. Role para baixo, selecione **Aceito para atualizações atuais e futuras** e selecione **Salvar**.

### Sobre esta tarefa

Em ambientes de produção, atualize o firmware em um nó de computação de cada vez.



O host ESXi deve ser retirado do modo de bloqueio antes de executar uma verificação de integridade e prosseguir com a atualização do firmware. ["Como desativar o modo de bloqueio no host ESXi"](#) Consulte e ["Comportamento do modo de bloqueio VMware"](#) para obter mais informações.

Para atualizações de UI ou API de controle de nuvem híbrida do NetApp, seu host ESXi será automaticamente colocado no modo de manutenção durante o processo de atualização se você tiver o

recurso DRS e o licenciamento necessário. O nó será reinicializado e após o processo de atualização estar concluído, o host ESXi será retirado do modo de manutenção. Para as opções de interface do usuário USB e BMC, você precisará colocar o host ESXi no modo de manutenção manualmente, conforme descrito em cada procedimento.



Antes de atualizar, verifique a versão atual do driver ESXi. Se o driver estiver desatualizado, atualize o driver primeiro. Em seguida, atualize o firmware de computação para seus nós de computação.

### Opções de atualização

Escolha a opção relevante para o seu cenário de atualização:

- [Use a IU do Controle de nuvem híbrida da NetApp para atualizar um nó de computação](#) (Recomendado)
- [Use a API de controle de nuvem híbrida da NetApp para atualizar um nó de computação](#)
- [Use uma unidade USB com o pacote de firmware de computação mais recente](#)
- [Utilizar a interface de utilizador \(UI\) do controlador de gestão de base \(BMC\)](#)

### Use a IU do Controle de nuvem híbrida da NetApp para atualizar um nó de computação

A partir dos serviços de gerenciamento 2,14, você pode atualizar um nó de computação usando a IU do Controle de nuvem híbrida da NetApp. Na lista de nós, você deve selecionar o nó a ser atualizado. A guia **Current Versions** mostra as versões atuais do firmware e a guia **proposed Versions** mostra as versões de atualização disponíveis, se houver.



Para uma atualização bem-sucedida, certifique-se de que a verificação de integridade no cluster do vSphere seja bem-sucedida.



A atualização da NIC, BIOS e BMC pode levar aproximadamente 60 minutos por nó, dependendo da velocidade de conectividade de rede entre o nó de gerenciamento e o host BMC.



O uso da IU de controle de nuvem híbrida da NetApp para atualizar o firmware de computação em nós de computação H300E/H500E/H700E não é mais compatível. Para atualizar, você deve usar um [Unidade USB](#) ou o [IU do BMC](#) para montar o pacote de firmware de computação.

### O que você vai precisar

- Se o nó de gerenciamento não estiver conectado à Internet, você baixou o pacote de firmware de computação do ["Site de suporte da NetApp"](#).



Você deve extrair o TAR.GZ arquivo para um TAR arquivo e, em seguida, extrair o TAR arquivo para o pacote de firmware de computação.

### Passos

1. Abra o endereço IP do nó de gerenciamento em um navegador da Web:

```
https://<ManagementNodeIP>
```

2. Faça login no controle de nuvem híbrida da NetApp fornecendo as credenciais de administrador do cluster de storage.

3. Selecione **Upgrade** perto do canto superior direito da interface.
4. Na página **Upgrades**, selecione **Compute firmware**.
5. Selecione o cluster que está a atualizar.

Você verá os nós no cluster listados juntamente com as versões atuais do firmware e versões mais recentes, se disponíveis para atualização.

6. Selecione **Procurar** para carregar o pacote de firmware de computação que você baixou do ["Site de suporte da NetApp"](#).
7. Aguarde até que o upload seja concluído. Uma barra de progresso mostra o status do upload.



O upload do arquivo acontecerá em segundo plano se você navegar para longe da janela do navegador.

É apresentada uma mensagem no ecrã depois de o ficheiro ser carregado e validado com êxito. A validação pode demorar vários minutos.

8. Selecione o pacote de firmware de computação.
9. Selecione **Begin Upgrade**.

Depois de selecionar **Begin Upgrade** (Iniciar atualização), a janela mostra as verificações de integridade falhadas, se houver.



A atualização não pode ser pausada depois de começar. O firmware será atualizado sequencialmente na seguinte ordem: NIC, BIOS e BMC. Não efetue login na IU do BMC durante a atualização. O login no BMC termina a sessão de controle de nuvem híbrida Serial-over-laN (sol) que monitora o processo de atualização.

10. Se as verificações de integridade no nível do cluster ou do nó forem aprovadas com avisos, mas sem falhas críticas, você verá **Pronto para ser atualizado**. Selecione **Upgrade Node**.



Enquanto a atualização estiver em andamento, você pode sair da página e voltar a ela mais tarde para continuar monitorando o progresso. Durante a atualização, a IU mostra várias mensagens sobre o status da atualização.



Durante a atualização do firmware nos nós de computação H610C e H615C, não abra o console Serial-over-laN (sol) por meio da IU da Web do BMC. Isso pode fazer com que a atualização falhe.

A IU exibe uma mensagem após a conclusão da atualização. Pode transferir registos após a conclusão da atualização. Para obter informações sobre as várias alterações de status de atualização, [Alterações de status da atualização](#) consulte .



Se ocorrer uma falha durante a atualização, o Controle de nuvem híbrida da NetApp reiniciará o nó, retirá-lo do modo de manutenção e exibirá o status da falha com um link para o log de erro. Você pode baixar o log de erros, que contém instruções específicas ou links para artigos da KB, para diagnosticar e corrigir qualquer problema. Para obter informações adicionais sobre problemas de atualização de firmware de nós de computação usando o Controle de nuvem híbrida da NetApp, consulte ["KB"](#) este artigo.

## Alterações de status da atualização

Aqui estão os diferentes estados que a IU mostra antes, durante e após o processo de atualização:

Estado de atualização	Descrição
Falha no nó em uma ou mais verificações de integridade. Expanda para ver detalhes.	Uma ou mais verificações de integridade falharam.
Erro	Ocorreu um erro durante a atualização. Você pode baixar o log de erros e enviá-lo para o suporte da NetApp.
Não foi possível detetar	Esse status será exibido se o Controle de nuvem híbrida da NetApp não puder consultar o nó de computação quando o ativo do nó de computação não tiver a tag de hardware.
Pronto para ser atualizado.	Todas as verificações de integridade passaram com êxito e o nó está pronto para ser atualizado.
Ocorreu um erro durante a atualização.	A atualização falha com esta notificação quando ocorre um erro crítico. Faça o download dos logs selecionando o link <b>Download Logs</b> para ajudar a resolver o erro. Você pode tentar atualizar novamente depois de resolver o erro.
A atualização do nó está em andamento.	A atualização está em andamento. Uma barra de progresso mostra o status da atualização.

## Use a API de controle de nuvem híbrida da NetApp para atualizar um nó de computação

Você pode usar APIs para atualizar cada nó de computação em um cluster para a versão de firmware mais recente. Você pode usar uma ferramenta de automação de sua escolha para executar as APIs. O fluxo de trabalho da API documentado aqui usa a IU da API REST disponível no nó de gerenciamento como exemplo.



O uso da IU de controle de nuvem híbrida da NetApp para atualizar o firmware de computação em nós de computação H300E/H500E/H700E não é mais compatível. Para atualizar, você deve usar um [Unidade USB](#) ou o [IU do BMC](#) para montar o pacote de firmware de computação.

### O que você vai precisar

Os ativos de nós de computação, incluindo o vCenter e os ativos de hardware, devem ser conhecidos pelos ativos de nós de gerenciamento. Você pode usar as APIs do serviço de inventário para verificar ativos (<https://<ManagementNodeIP>/inventory/1/>).

### Passos

1. Vá para o software NetApp HCI "[página de download](#)" e faça o download do pacote de firmware de computação mais recente para um dispositivo acessível ao nó de gerenciamento.
2. Faça o upload do pacote de firmware de computação para o nó de gerenciamento:
  - a. Abra a IU da API REST do nó de gerenciamento no nó de gerenciamento:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
    - i. Introduza o nome de utilizador e a palavra-passe do cluster.
    - ii. Introduza a ID do cliente como `mnode-client`.
    - iii. Selecione **autorizar** para iniciar uma sessão.
    - iv. Feche a janela autorização.
  - c. Na IU da API REST, selecione **POST /packages**.
  - d. Selecione **Experimente**.
  - e. Selecione **Procurar** e selecione o pacote de firmware de computação.
  - f. Selecione **execute** para iniciar o upload.
  - g. Na resposta, copie e salve o ID do pacote de firmware de computação ("`id`") para uso em uma etapa posterior.
3. Verifique o status do upload.
- a. Na IU da API REST, selecione **GET /packages/ id/status**.
  - b. Selecione **Experimente**.
  - c. Insira o ID do pacote de firmware de computação que você copiou na etapa anterior em **id**.
  - d. Selecione **execute** para iniciar a solicitação de status.

A resposta indica `state` como `SUCCESS` quando concluída.

- e. Na resposta, copie e salve o nome do pacote de firmware de computação ("`name`") e a versão ("`version`") para uso em uma etapa posterior.
4. Localize o ID do controlador de computação e o ID do hardware do nó que você pretende atualizar:
- a. Abra a IU da API REST do serviço de inventário no nó de gerenciamento:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Selecione **autorizar** e preencha o seguinte:
  - i. Introduza o nome de utilizador e a palavra-passe do cluster.
  - ii. Introduza a ID do cliente como `mnode-client`.
  - iii. Selecione **autorizar** para iniciar uma sessão.
  - iv. Feche a janela autorização.
- c. Na IU da API REST, selecione **GET /installations**.
- d. Selecione **Experimente**.
- e. Selecione **Executar**.
- f. Na resposta, copie o ID do ativo de instalação ("`id`").
- g. Na IU da API REST, selecione **\*GET /installations/**
- h. Selecione **Experimente**.
- i. Cole o ID do ativo de instalação no campo **id**.
- j. Selecione **Executar**.

- k. Na resposta, copie e salve o ID do controlador do cluster ("controllerId") e o ID do hardware do nó ("hardwareId") para uso em uma etapa posterior:

```
"compute": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterId": "Test-1B",
        "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
```

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.111.0.111",
      "credentialsAvailable": true,
      "credentialsValidated": true
    },
    "chassisSerialNumber": "111930011231",
    "chassisSlot": "D",
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",
    "model": "H410C",
```

5. Execute a atualização do firmware do nó de computação:

- a. Abra a IU da API REST do serviço de hardware no nó de gerenciamento:

```
https://<ManagementNodeIP>/hardware/2/
```

- b. Selecione **autorizar** e preencha o seguinte:

- i. Introduza o nome de utilizador e a palavra-passe do cluster.
- ii. Introduza a ID do cliente como `mnode-client`.
- iii. Selecione **autorizar** para iniciar uma sessão.
- iv. Feche a janela autorização.

- c. Selecione **POST /nodes/(hardware\_id)/Upgrades**.

- d. Selecione **Experimente**.

- e. Insira o ID do ativo do host de hardware ("hardwareId" salvo de uma etapa anterior) no campo parâmetro.

- f. Faça o seguinte com os valores de carga útil:

- i. Guarde os valores `"force": false` e `"maintenanceMode": true` de modo que as

verificações de integridade sejam executadas no nó e o host ESXi seja definido para o modo de manutenção.

- ii. Introduza a ID do controlador do cluster ("controllerId" guardada a partir de um passo anterior).
- iii. Insira o nome e a versão do pacote de firmware de computação que você salvou de uma etapa anterior.

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

- g. Selecione **execute** para iniciar a atualização.



A atualização não pode ser pausada depois de começar. O firmware será atualizado sequencialmente na seguinte ordem: NIC, BIOS e BMC. Não efetue login na IU do BMC durante a atualização. O login no BMC termina a sessão de controle de nuvem híbrida Serial-over-laN (sol) que monitora o processo de atualização.

- h. Copie o ID da tarefa de atualização que faz parte do ("resourceLink" URL do link de recurso ) na resposta.

6. Verifique o progresso e os resultados da atualização:

- a. Selecione **GET /task//log**.
- b. Selecione **Experimente**.
- c. Insira o ID da tarefa da etapa anterior em **Task\_ID**.
- d. Selecione **Executar**.
- e. Siga um destes procedimentos se houver problemas ou requisitos especiais durante a atualização:

Opção	Passos
Você precisa corrigir problemas de integridade do cluster devido a failedHealthChecks mensagem no corpo de resposta.	<ol style="list-style-type: none"><li>i. Vá para o artigo específico da KB listado para cada problema ou execute o recurso especificado.</li><li>ii. Se um KB for especificado, conclua o processo descrito no artigo da KB relevante.</li><li>iii. Depois de resolver problemas de cluster, reautentique se necessário e selecione <b>POST /nodes/ hardware_id/Upgrades</b>.</li><li>iv. Repita as etapas conforme descrito anteriormente na etapa de atualização.</li></ol>

Opção	Passos
A atualização falha e as etapas de mitigação não estão listadas no log de atualização.	i. Veja isto <a href="#">"Artigo da KB"</a> (login necessário).

- f. Execute a API `get /task/_id/logs` várias vezes, conforme necessário, até que o processo esteja concluído.

Durante a atualização, o `status` indica `running` se não foram encontrados erros. À medida que cada etapa termina, o `status` valor muda para `completed`.

A atualização foi concluída com êxito quando o `status` de cada etapa é `completed` e o `percentageCompleted` valor é 100.

7. (Opcional) confirmar versões de firmware atualizadas para cada componente:

- a. Abra a IU da API REST do serviço de hardware no nó de gerenciamento:

```
https://<ManagementNodeIP>/hardware/2/
```

- b. Selecione **autorizar** e preencha o seguinte:

- i. Introduza o nome de utilizador e a palavra-passe do cluster.
- ii. Introduza a ID do cliente como `mnode-client`.
- iii. Selecione **autorizar** para iniciar uma sessão.
- iv. Feche a janela autorização.

- c. Na IU da API REST, selecione **GET /nodes/ hardware\_id/Upgrades**.

- d. (Opcional) Digite os parâmetros de `data` e `status` para filtrar os resultados.

- e. Insira o ID do ativo do host de hardware ("`hardwareId`" salvo de uma etapa anterior) no campo parâmetro.

- f. Selecione **Experimente**.

- g. Selecione **Executar**.

- h. Verifique na resposta se o firmware para todos os componentes foi atualizado com êxito da versão anterior para o firmware mais recente.

### Use uma unidade USB com o pacote de firmware de computação mais recente

Você pode inserir uma unidade USB com o pacote de firmware de computação mais recente baixado em uma porta USB no nó de computação. Como alternativa ao uso do método de pen drive USB descrito neste procedimento, você pode montar o pacote de firmware de computação no nó de computação usando a opção **Virtual CD/DVD** no console virtual na interface do controlador de gerenciamento de placa de base (BMC). O método BMC leva consideravelmente mais tempo do que o método USB pen drive. Certifique-se de que a sua estação de trabalho ou servidor tem a largura de banda de rede necessária e de que a sessão do navegador com o BMC não expira.

### O que você vai precisar

- Se o nó de gerenciamento não estiver conectado à Internet, você baixou o pacote de firmware de computação do ["Site de suporte da NetApp"](#).



Você deve extrair o TAR.GZ arquivo para um TAR arquivo e, em seguida, extrair o TAR arquivo para o pacote de firmware de computação.

## Passos

1. Use o utilitário Etcher para flash o pacote de firmware de computação para uma unidade USB.
2. Coloque o nó de computação no modo de manutenção usando o VMware vCenter e evacue todas as máquinas virtuais do host.



Se o VMware Distributed Resource Scheduler (DRS) estiver habilitado no cluster (esse é o padrão nas instalações do NetApp HCI), as máquinas virtuais serão migradas automaticamente para outros nós no cluster.

3. Insira a pen drive USB em uma porta USB no nó de computação e reinicie o nó de computação usando o VMware vCenter.
4. Durante o ciclo PÓS DO nó de computação, pressione **F11** para abrir o Gerenciador de Inicialização. Você pode precisar pressionar **F11** várias vezes em sucessão rápida. Pode efetuar esta operação ligando um vídeo/teclado ou utilizando a consola no BMC.
5. Selecione **One Shot > USB Flash Drive** no menu que aparece. Se a pen USB não aparecer no menu, verifique se a unidade flash USB faz parte da ordem de inicialização herdada no BIOS do sistema.
6. Pressione **Enter** para inicializar o sistema a partir da unidade USB. O processo de flash do firmware é iniciado.

Depois que o firmware piscar estiver concluído e o nó reiniciar, pode demorar alguns minutos para o ESXi iniciar.

7. Depois que a reinicialização estiver concluída, saia do modo de manutenção no nó de computação atualizado usando o vCenter.
8. Remova a unidade flash USB do nó de computação atualizado.
9. Repita essa tarefa para outros nós de computação no cluster ESXi até que todos os nós de computação sejam atualizados.

## Utilizar a interface de utilizador (UI) do controlador de gestão de base (BMC)

Você deve executar as etapas sequenciais para carregar o pacote de firmware de computação e reinicializar o nó para o pacote de firmware de computação para garantir que a atualização seja bem-sucedida. O pacote de firmware de computação deve estar localizado no sistema ou na máquina virtual (VM) que hospeda o navegador da Web. Verifique se você baixou o pacote de firmware de computação antes de iniciar o processo.



A recomendação é ter o sistema ou VM e o nó na mesma rede.



Demora aproximadamente 25 a 30 minutos para a atualização através da IU do BMC.

- [Atualize o firmware nos nós H410C e H300E/H500E/H700E](#)
- [Atualize o firmware em nós H610C/H615C](#)

### Atualize o firmware nos nós H410C e H300E/H500E/H700E

Se o nó fizer parte de um cluster, você deve colocar o nó no modo de manutenção antes da atualização e

retirá-lo do modo de manutenção após a atualização.



Ignore a seguinte mensagem informativa que você vê durante o processo: Untrusty Debug Firmware Key is used, SecureFlash is currently in Debug Mode

## Passos

1. Se o nó fizer parte de um cluster, coloque-o no modo de manutenção da seguinte forma. Caso contrário, vá para o passo 2.
  - a. Faça login no cliente da Web do VMware vCenter.
  - b. Clique com o botão direito do rato no nome do host (nó de computação) e selecione **Maintenance Mode (modo de manutenção) > Enter Maintenance Mode (entrar no modo de manutenção)**.
  - c. Selecione **OK**. As VMs no host serão migradas para outro host disponível. A migração de VM pode levar tempo, dependendo do número de VMs que precisam ser migradas.



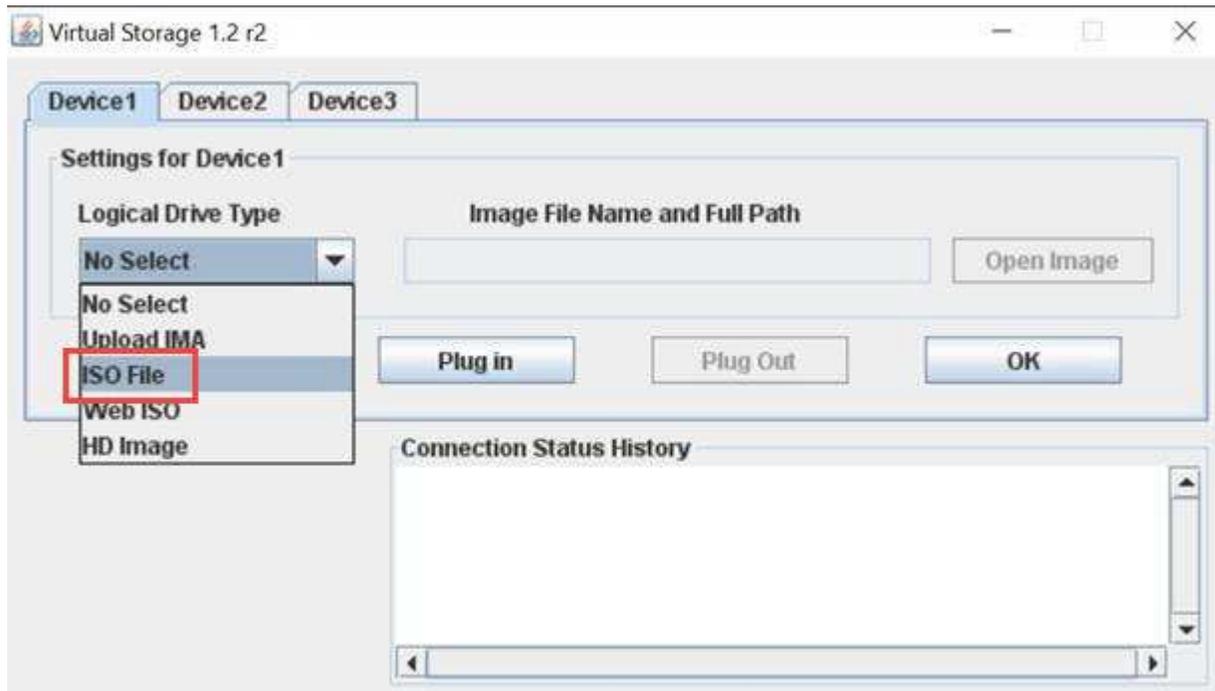
Certifique-se de que todas as VMs no host sejam migradas antes de prosseguir.

2. Navegue até a IU do BMC, <https://BMCIP/#login>, em que BMCIP é o endereço IP do BMC.
3. Faça login usando suas credenciais.
4. Selecione **Remote Control > Console Redirection** (controlo remoto > Redirecionamento da consola).
5. Selecione **Launch Console**.



Você pode ter que instalar o Java ou atualizá-lo.

6. Quando o console for aberto, selecione **Virtual Media > Virtual Storage**.
7. Na tela **Virtual Storage**, selecione **Logical Drive Type** e **ISO File**.



8. Selecione **Open Image** (abrir imagem) para navegar até a pasta onde você baixou o arquivo do pacote de firmware de computação e selecione o arquivo do pacote de firmware de computação.

9. Selecione **Plug in**.
10. Quando o status da conexão for exibido `Device#: VM Plug-in OK!!`, selecione **OK**.
11. Reinicie o nó pressionando **F12** e selecionando **Restart** ou selecionando **Power Control > Set Power Reset**.
12. Durante a reinicialização, pressione **F11** para selecionar as opções de inicialização e carregar o pacote de firmware de computação. Você pode ter que pressionar F11 algumas vezes antes que o menu de inicialização seja exibido.

Você verá a seguinte tela:

```
ISOLINUX 6.84 6.84-pre1 ETCD Copyright (C) 1994-2015 H.
Enber Linux Installation LiveCD

Enter to boot: F1 for kernels  F2 for options.
Booting enber
boot:
```

13. Na tela acima, pressione **Enter**. Dependendo da sua rede, pode demorar alguns minutos depois de premir **Enter** para iniciar a atualização.



Algumas atualizações de firmware podem fazer com que o console se desconete e/ou faça com que sua sessão no BMC se desconete. Você pode fazer login novamente no BMC, no entanto, alguns serviços, como o console, podem não estar disponíveis devido às atualizações de firmware. Após a conclusão das atualizações, o nó executará uma reinicialização a frio, o que pode levar aproximadamente cinco minutos.

14. Faça login novamente na IU do BMC e selecione **sistema** para verificar a versão do BIOS e o tempo de compilação após a inicialização no sistema operacional. Se a atualização foi concluída corretamente, você verá as novas versões do BIOS e do BMC.



A versão do BIOS não mostrará a versão atualizada até que o nó tenha terminado totalmente a inicialização.

15. Se o nó fizer parte de um cluster, execute as etapas abaixo. Se for um nó autônomo, nenhuma ação adicional será necessária.
  - a. Faça login no cliente da Web do VMware vCenter.
  - b. Retire o host do modo de manutenção. Isso pode mostrar um sinalizador vermelho desconetado. Aguarde até que todos os Estados sejam apagados.
  - c. Ligue qualquer uma das VMs restantes que foram desligadas.

#### Atualize o firmware em nós H610C/H615C

As etapas variam dependendo se o nó é autônomo ou parte de um cluster. O procedimento pode levar aproximadamente 25 minutos e inclui desligar o nó, carregar o pacote de firmware de computação, piscar os dispositivos e ligar o nó novamente após a atualização.

#### Passos

1. Se o nó fizer parte de um cluster, coloque-o no modo de manutenção da seguinte forma. Caso contrário, vá para o passo 2.

- a. Faça login no cliente da Web do VMware vCenter.
- b. Clique com o botão direito do rato no nome do host (nó de computação) e selecione **Maintenance Mode (modo de manutenção) > Enter Maintenance Mode (entrar no modo de manutenção)**.
- c. Selecione **OK**. As VMs no host serão migradas para outro host disponível. A migração de VM pode levar tempo, dependendo do número de VMs que precisam ser migradas.

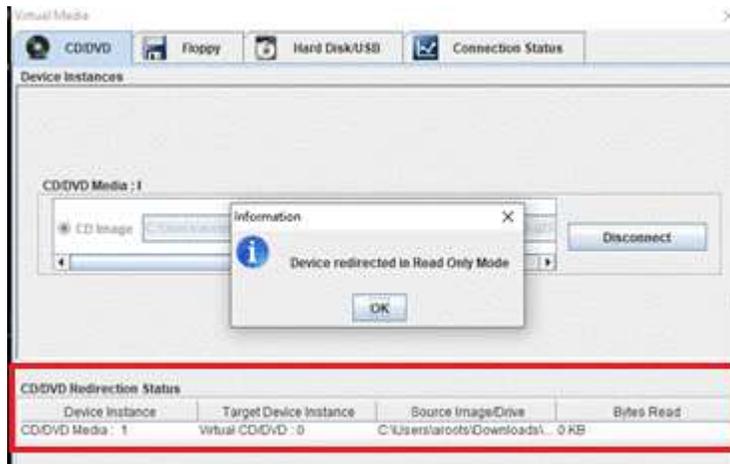


Certifique-se de que todas as VMs no host sejam migradas antes de prosseguir.

2. Navegue até a IU do BMC <https://BMCIP/#login> , em que BMC IP é o endereço IP do BMC.
3. Faça login usando suas credenciais.
4. Selecione **Controle remoto > inicie o KVM (Java)**.
5. Na janela do console, selecione **Mídia > Virtual Media Wizard**.



6. Selecione **Procurar** e selecione o ficheiro de firmware de computação .iso.
7. Selecione **Connect**. Um pop-up indicando sucesso é exibido, juntamente com o caminho e o dispositivo que aparece na parte inferior. Você pode fechar a janela **Virtual Media**.



8. Reinicie o nó pressionando **F12** e selecionando **Restart** ou selecionando **Power Control > Set Power Reset**.
9. Durante a reinicialização, pressione **F11** para selecionar as opções de inicialização e carregar o pacote de firmware de computação.
10. Selecione **AMI Virtual CDROM** na lista exibida e selecione **Enter**. Se você não vir o CDROM virtual AMI na lista, vá para o BIOS e ative-o na lista de inicialização. O nó será reinicializado após você salvar. Durante a reinicialização, pressione **F11**.



11. No ecrã apresentado, seleccione **Enter**.



Algumas atualizações de firmware podem fazer com que o console se desconete e/ou faça com que sua sessão no BMC se desconete. Você pode fazer login novamente no BMC, no entanto, alguns serviços, como o console, podem não estar disponíveis devido às atualizações de firmware. Após a conclusão das atualizações, o nó executará uma reinicialização a frio, o que pode levar aproximadamente cinco minutos.

12. Se você for desconectado do console, seleccione **Controle remoto** e seleccione **Launch KVM** ou **Launch KVM (Java)** para reconectar e verificar quando o nó tiver terminado de inicializar o backup. Você pode precisar de várias reconexões para verificar se o nó foi inicializado com sucesso.



Durante o processo de ativação, por aproximadamente cinco minutos, o console KVM exibe **sem sinal**.

13. Depois que o nó estiver ligado, seleccione **Painel > informações do dispositivo > mais informações** para verificar as versões do BIOS e do BMC. As versões atualizadas do BIOS e do BMC são exibidas. A versão atualizada do BIOS não será exibida até que o nó tenha sido totalmente inicializado.
14. Se você colocou o nó no modo de manutenção, depois que o nó inicializar para ESXi, clique com o botão direito do Mouse no nome do host (nó de computação) e seleccione **modo de manutenção > Sair do modo de manutenção** e migre as VMs de volta para o host.
15. No vCenter, com o nome do host seleccionado, configure e verifique a versão do BIOS.

### Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)

## Automatize as atualizações de firmware de nós de computação com o Ansible

Você pode atualizar o firmware do sistema em nós de computação do NetApp HCI, incluindo firmware para componentes como BMC, BIOS e NIC usando fluxos de trabalho no Controle de nuvem híbrida do NetApp. Para instalações com grandes clusters de computação, é possível automatizar os fluxos de trabalho com o Ansible para realizar

uma atualização progressiva de todo o cluster.



Embora a função Ansible para automatizar as atualizações de firmware de nós de computação seja disponibilizada pelo NetApp, a automação é um componente auxiliar que requer configuração adicional e a execução de componentes de software. A modificação da automação do Ansible é suportada apenas no melhor esforço.



A função Ansible para upgrades funciona apenas nos nós de computação da série H da NetApp HCI. Você não pode usar essa função para atualizar nós de computação de terceiros.

### O que você vai precisar

- **Disponibilidade e pré-requisitos para atualizações de firmware:** A instalação do NetApp HCI deve estar pronta para atualização de firmware, conforme descrito nas instruções do "[a efetuar atualizações de firmware](#)".
- **Prontidão para executar a automação no nó de controle do Ansible:** Um servidor físico ou virtual para executar a automação de atualizações de firmware no Ansible.

### Sobre esta tarefa

Em um ambiente de produção, você deve atualizar os nós de computação em um cluster em uma instalação do NetApp HCI de forma contínua; um nó após o outro, um nó de cada vez. Orquestre o processo geral de atualização do firmware do nó de computação para um único nó de computação, incluindo a execução de verificações de integridade, colocação do ESXi nos nós de computação em manutenção e reinicialização do nó de computação para aplicar as atualizações de firmware NetApp. A função Ansible oferece a opção de orquestrar a atualização de firmware para um grupo de nós de computação ou clusters inteiros.

### Comece a usar a automação de atualização de firmware

Para começar, navegue até o "[Repositório do NetApp Ansible no GitHub](#)" e faça o download da `nar_compute_nodes_firmware_upgrades` função e da documentação.

### Encontre mais informações

- "[Página de recursos do NetApp HCI](#)"

## Atualize seus componentes vSphere para um sistema NetApp HCI com o plug-in Element para vCenter Server

Quando você atualiza os componentes do VMware vSphere da instalação do NetApp HCI, há algumas etapas adicionais que você precisará executar para o plug-in Element para vCenter Server.

### Passos

1. Para atualizações do vCSA, "[limpar](#)" as configurações do QoSSIOC no plug-in (**Configuração do NetApp Element > Configurações do QoSSIOC**). O campo **Status do QoSSIOC** é exibido `Not Configured` após o processo estar concluído.
2. Para atualizações do vCSA e do Windows, "[anular registro](#)" o plug-in do vCenter Server ao qual ele está associado usando o utilitário de Registro.
3. "[Atualize o vSphere, incluindo vCenter Server, ESXi, VMs e outros componentes VMware](#)".



Você deve atualizar para o plug-in do NetApp Element para vCenter Server 5,0 ou posterior para oferecer a capacidade de implantar o plug-in com o VMware vCenter 7,0 Update 3 sem precisar aplicar uma solução alternativa.



Com o Element Plug-in para vCenter Server 4.x, quando você atualiza para o VMware vCenter Server 7,0 Update 3, o plug-in não consegue implantar. Para resolver esse problema usando o Spring Framework 4, ["Este artigo da KB"](#) consulte .

Ao atualizar o ESXi para nós de computação para um ["cluster de dois nós"](#), atualize apenas um nó de computação de cada vez para que apenas um nó de testemunha fique temporariamente indisponível e o quorum do cluster possa ser mantido.

4. ["Registe-se"](#) O plug-in Element para vCenter Server novamente com o vCenter.
5. ["Adicionar clusters"](#) utilizar o plug-in.
6. ["Configure as configurações do QoSSIOC"](#) utilizar o plug-in.
7. ["Ative o QoSSIOC"](#) para todos os datastores controlados pelo plug-in.

## Encontre mais informações

- ["Plug-in do NetApp Element para vCenter Server"](#)
- ["Página de recursos do NetApp HCI"](#)
- ["Relatório técnico de clusters de storage de dois nós da NetApp HCI"](#)

## **Informações sobre direitos autorais**

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.